Образовательная автономная некоммерческая организация высшего образования

«МОСКОВСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ»

Программа СПО по профессии 080203.01	**38.01.01**	**Оператор диспетчерской (производственно-диспетчерской) службы**
	(код)	*(наименование)*

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И СЕТЕЙ В АО «СИСТЕМНЫЙ ОПЕРАТОР ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ»

Обучающийся Мамонтов Илья Васильевич
(Ф.И.О. полностью) *подпись*

Руководитель Мащенко Татьяна Павловна
(Ф.И.О. полностью) *подпись*

МОСКВА 2025 г.

Образовательная автономная некоммерческая организация высшего образования

«МОСКОВСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ»

ЗАДАНИЕ

на выпускную квалификационную работу

обучающийся Мамонтов Илья Васильевич

1. Тема: Направления совершенствования информационной безопасности автоматизированных систем и сетей в АО «Системный оператор Единой энергетической системы»

2. Срок сдачи обучающимся законченной работы «16» июля 2025 г.

3. Исходные данные к выпускной квалификационной работе: научная и учебная литература, интернет ресурсы.

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов):

ВВЕДЕНИЕ
Глава 1. ТЕОРЕТИЧЕСКИЕ ОСНОВНЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И СЕТЕЙ
1.1. Понятие и сущность информационной безопасности автоматизированных систем и сетей на предприятии
1.2. Нормативное регулирование обеспечения информационной безопасности автоматизированных систем и сетей на предприятии
1.3. Комплексное обеспечение информационной безопасности автоматизированных систем и сетей на предприятии
Глава 2. НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И СЕТЕЙ В АО «СИСТЕМНЫЙ ОПЕРАТОР ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ»
2.1. Организационная и финансовая характеристика АО «Системный оператор Единой энергетической системы»
2.2. Анализ угроз и уязвимостей компании, выявление проблем
2.3. Предложения с экономическим обоснованием по совершенствованию информационной безопасности автоматизированных систем и сетей в АО «Системный оператор Единой энергетической системы»
ЗАКЛЮЧЕНИЕ
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ
ПРИЛОЖЕНИЯ

Дата выдачи задания __.__.202__ Задание принял (дата) __.__.202__

Подпись руководителя ____________ Подпись обучающегося____________

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Направления совершенствования информационной безопасности автоматизированных систем и сетей в АО «Системный оператор Единой энергетической системы» является актуальной темой исследования с учетом импортозамещения как основного направления в системе обеспечения информационной безопасности в электроэнергетической компании по нескольким причинам.

Во-первых, обеспечение кибербезопасности в электроэнергетике становится все более важной задачей. С увеличением числа кибератак и угроз кибербезопасности важно иметь собственные, надежные системы межсетевого экранирования, которые не зависят от импортных решений. Это помогает уменьшить уязвимость системы к внешним атакам и обеспечивает надежную защиту от утечек данных или недоступности энергосистемы.

Во-вторых, импортозамещение в данной области может способствовать развитию отечественной индустрии информационной безопасности. Создание и поддержка собственных технологий межсетевого экранирования способствует росту отечественных производителей, что в свою очередь создает новые рабочие места и способствует экономическому развитию.

Наконец, управление электроэнергетической системой требует высокой степени надежности и эффективности. Импортозамещение в области межсетевого экранирования позволяет компании иметь более прямой контроль над обновлениями, технической поддержкой и адаптацией

системы под конкретные требования, что в конечном итоге способствует стабильной и более эффективной работе электроэнергетической системы.

При таких ограничениях и запретах на использование иностранного программного обеспечения на значимых объектах критической информационной инфраструктуры России согласно указа Президент РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ" [1], важным становится использование отечественных решений, в том числе систем межсетевого экранирования (МСЭ).

Для энергетических компаний, важных объектов критической информационной инфраструктуры, будет целесообразным рассмотрение отечественных МСЭ-решений. При выборе системы следует учитывать не только технические характеристики, но и соответствие стандартам безопасности и сертификациям, а также обновления и поддержку отечественных поставщиков.

Такие меры направлены на обеспечение технологической независимости и повышение кибербезопасности стратегически важных объектов.

В качестве объекта исследования в работе выступает электроэнергетическое предприятие.

В качестве предмета исследования рассматривается процесс по выбору системе межсетевого экранирования для защиты информации на рабочих местах в корпоративной сети предприятия.

Целью предоставленной работы является исследование направлений совершенствования информационной

безопасности автоматизированных систем и сетей в АО «Системный оператор Единой энергетической системы».

Для достижения заданной цели необходимо выполнить ряд задач:

- провести техническую и экономическую характеристику предметной области рассматриваемого предприятия;

- проанализировать риски информационной безопасности (ИБ) предприятия;

- дать характеристику комплексу задач, задаче и обоснованию необходимости в усовершенствовании системы межсетевого экранирования на рассматриваемом предприятии;

- произвести анализ, выбор и описание внедрения отечественных систем межсетевого экранирования;

- обосновать экономическую эффективность разработанного проекта.

При написании проекта применялись такие способы научного исследования: изучение нормативно-правовой базы, научной литературы по теме исследования, сравнительный и аналитический способы.

В качестве эмпирической базы исследования послужило изучение главных принципов изучения способов определения угроз и уязвимостей предприятия в целях защиты информации от несанкционированного доступа.

В качестве основы работы послужили всевозможные источники информации по защите компьютерных сетей: нормативные документы, периодические издания, учебная и научная литература зарубежных и отечественных авторов, электронные ресурсы.

Глава 1. ТЕОРЕТИЧЕСКИЕ ОСНОВНЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И СЕТЕЙ

1.1. Понятие и сущность информационной безопасности автоматизированных систем и сетей на предприятии

Обеспечение конфиденциальности, целостности и доступности информации на предприятии - основная задача СЗИ.

Под конфиденциальностью следует понимать, что доступ к информации имеет только определенный круг лиц, при этом возможно разграничение доступа к информации между сотрудниками.

Целостность подразумевает под собой, что только определенный круг лиц имеет право изменять информацию.

Доступность – свойство, гарантирующее, что лица, имеющие доступ к информации в нужный момент, смогут получить доступ.

Система защиты информации представляет собой многофункциональный инструмент, с помощью которого должна обеспечиваться безопасность ИС.

СЗИ управляется с помощью администраторов сети, которые выполняют следующие функции [5]:

- установка и настройка сетевых узлов;
- поиск неисправностей;
- мониторинг сетевого трафика;
- настройка и обслуживание ПО;

- обеспечение защиты данных;
- планирование сети;
- установка и настройка сетевых служб;
- установка и настройка сетевых протоколов.

Обеспечивать стабильную и бесперебойную работу предприятия помогает корпоративная сеть, с помощью которой происходит объединение всех работников, которым необходим доступ к информационной системе предприятия.

Сложные, требующие высокой точности и бесперебойности процессы, которые происходят на предприятии влияют на безопасность деятельности. Неотъемлемая часть процесса – информационное взаимодействие между всеми участниками, которые пользуются информационными системами.

Согласно [8] к целям защиты информации относятся:

- предотвращение утечки, хищения, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима как объекта собственности;
- защита конституционных прав граждан по сохранению личной тайны, конфиденциальности персональных данных, имеющихся в информационных системах;

- сохранение коммерческой тайны, конфиденциальности документированной информации в соответствии с законодательством;

- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Система защиты информации предназначена обеспечивать безопасность всей защищаемой информации. В связи с этим к ней должны предъявляться следующие требования:

- она должна быть привязана к целям и задачам защиты информации на предприятии;

- должна учитывать все объекты защиты, все обстоятельства и факторы, влияющие на безопасность информации;

- должна базироваться на принципе гарантированного результата;

- должна быть «вмонтированной» в технологические схемы сбора, хранения, обработки, передачи и использования информации;

- должна быть технологически и экономически обоснованной;

- должна быть реализуемой, обеспеченной всеми необходимыми ресурсами;

- должна быть простой и удобной в эксплуатации;

- должна быть непрерывной;

- должна быть способной к целенаправленному приспособлению при изменении компонентов ее составных частей, технологии обработки информации, условий защиты.

Таким образом, проанализировав требования к СЗИ, можно сделать выводы, что безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.

1.2. Нормативное регулирование обеспечения информационной безопасности автоматизированных систем и сетей на предприятии

Обеспечение информационной безопасности автоматизированных систем и сетей на предприятиях в Российской Федерации регулируется обширным комплексом нормативных правовых актов, технических регламентов, государственных стандартов и методических рекомендаций. Нормативное регулирование в данной области основано на требованиях к защите информации, в том числе содержащей персональные данные, государственную тайну и иную охраняемую по закону информацию, а также на необходимости противодействия компьютерным инцидентам и киберугрозам [11, 16].

Ключевым документом, определяющим государственную политику в сфере ИБ, является Стратегия обеспечения информационной безопасности Российской Федерации, утверждённая Указом Президента РФ от 5 декабря 2016 г. № 646. В соответствии с положениями данной стратегии, предприятия, эксплуатирующие информационные системы, обязаны реализовывать организационные и технические меры защиты, направленные на обеспечение устойчивости и защищённости информационной инфраструктуры от

внутренних и внешних угроз.

Значительное место в правовом регулировании ИБ занимает Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", который устанавливает правовые основы хранения, обработки и защиты информации. В развитие его положений действует Федеральный закон от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", который обязывает субъекты КИИ (в том числе и коммерческие предприятия, соответствующие критериям значимости) реализовывать специальные меры защиты автоматизированных систем и сетей.

Особое значение придаётся требованиям Постановления Правительства РФ № 1119 от 1 ноября 2012 г., утверждающего правила по обеспечению безопасности персональных данных при их обработке в информационных системах, а также Постановления № 152, регламентирующего уровни защищённости таких систем. В техническом аспекте реализации защиты важную роль играют приказы ФСТЭК России, в частности, Приказ № 239 от 17 февраля 2021 г., который устанавливает требования к защите информации в государственных информационных системах и ИСПДн.

Важнейшими методическими документами являются руководства и базовые модели угроз, утверждаемые ФСТЭК и ФСБ России, включая Базовую модель угроз безопасности персональных данных, Методики определения актуальных угроз и профили защиты. Также активно используются стандарты серии ГОСТ Р ИСО/МЭК 27000, адаптированные к национальному контексту, в частности ГОСТ Р ИСО/МЭК

27001-2021, регламентирующий построение и сертификацию систем менеджмента информационной безопасности.

Таким образом, нормативно-правовая база в РФ формирует целостную и многоуровневую систему требований к обеспечению ИБ на всех этапах жизненного цикла автоматизированных систем и сетей. Соблюдение этих требований является обязательным как для государственных учреждений, так и для коммерческих организаций, что обусловлено высоким уровнем зависимости современного бизнеса от надёжности и защищённости информационных ресурсов.

1.3. Комплексное обеспечение информационной безопасности автоматизированных систем и сетей на предприятии

Выпускная квалификационная работа, направленная на создание устойчивой системы информационной безопасности, требует реализации последовательного комплекса мероприятий по защите информации и персональных данных. Процесс разработки системы информационной безопасности предполагает поэтапное выполнение ряда ключевых задач, включающих аудит, проектирование, внедрение, сопровождение и обслуживание.

Первоначальный этап аудита посвящен тщательному анализу и оценке текущего состояния системы информационной безопасности. В ходе аудита осуществляется выявление критически значимых объектов документооборота, потенциальных угроз и уязвимостей, а также проводится оценка рисков и возможного ущерба,

который может быть нанесён в случае реализации угроз. Этот этап играет ключевую роль в формировании базы для последующего проектирования системы [4].

На этапе проектирования разрабатываются концептуальные и регулятивные основы системы информационной безопасности. В первую очередь создаётся концепция информационной безопасности, которая определяет общие принципы и подходы к обеспечению безопасности данных. Далее формируется политика информационной безопасности, содержащая чётко прописанные правила и регламенты, обязательные к соблюдению всеми сотрудниками и участниками информационных процессов. Также разрабатываются различные регламенты, положения, инструкции, журналы и акты, которые детализируют процедуры обработки информации и управления безопасностью. Важным элементом проектирования является создание частной модели угроз безопасности персональных данных, которая, опираясь на специфику используемой информационной системы, позволяет идентифицировать потенциальные риски. Завершающим аспектом этого этапа становится определение объектов защиты информации, для которых, при необходимости, проводится тестирование на резервном оборудовании [9].

Этап внедрения включает в себя закупку и ввод в эксплуатацию необходимого технического, криптографического и программного обеспечения. В рамках этого этапа также осуществляется обучение сотрудников, которым предстоит работать с новыми средствами защиты информации, что позволяет обеспечить их эффективное

использование в рамках установленной системы.

Завершающий этап сопровождения и обслуживания направлен на обеспечение непрерывного и устойчивого функционирования системы информационной безопасности. Ответственные лица проводят плановые проверки, мониторинг состояния системы и оперативное устранение инцидентов, что способствует поддержанию высокого уровня защиты информации в долгосрочной перспективе.

В соответствии с рисунком 1 представлена схема цикла работ по обеспечению системы информационной безопасности [6].

Соблюдение цикла работ по обеспечению системы информационной безопасности (ИБ) способствует созданию многоэшелонированной защиты информации и персональных данных (ПДн).

В локальной вычислительной сети (ЛВС) организации циркулирует как пользовательская, так и служебная информация. Автоматизированные рабочие места (АРМ) генерируют потоки информации, связанные с электронным документооборотом, но средства электронной цифровой подписи не используются.

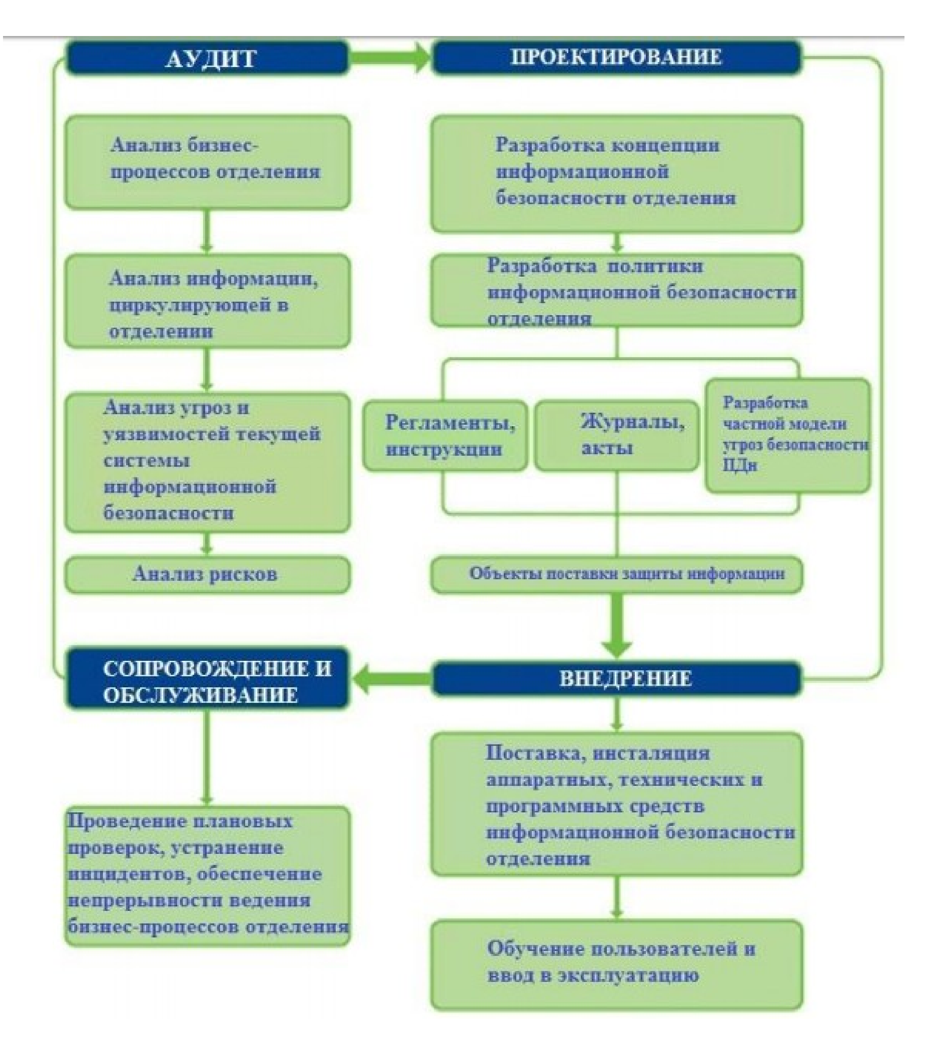


Рисунок 1 - Схема цикла работ по обеспечению системы ИБ

В организации информация делится на следующие типы [6]:

- почтовый трафик;

- файлы, связанные с коммерческой деятельностью;

- сетевой трафик, связанный с использованием ресурсов сети Интернет;

- служебный трафик в ЛВС;

- паразитный трафик, формируемый различными источниками.

С учетом бизнес-процессов в организации, требуется гарантировать заданную вероятность доступности, сохранности и конфиденциальности коммерческой тайны в

проектируемой ЛВС.

Взаимодействие с другими системами и точками входа в ЛВС организации осуществляется по следующим каналам:

- связь с сетью Интернет через линию связи;

- коммутируемый канал связи с использованием технологии GPRS.

Защита подключений к внешним сетям осуществляется с помощью встроенных средств защиты маршрутизатора. Доступ к информационным ресурсам сети Интернет открыт для всех пользователей ЛВС организации.

Политика информационной безопасности организации представляет собой комплексную систему, направленную на обеспечение защиты информации и персональных данных от различных угроз. Эта система включает в себя не только определение стратегических задач и целей в области безопасности, но и установление эффективных механизмов контроля и управления, обеспечивающих многоуровневую защиту информационных систем.

Важность обеспечения информационной безопасности обусловлена необходимостью защиты критически важных информационных ресурсов организации от потенциальных угроз, включая несанкционированный доступ, повреждение или утрату информации. Основной целью политики информационной безопасности является минимизация этих рисков, что достигается через разработку и внедрение мер, направленных на предотвращение возможных инцидентов, а также на снижение их последствий в случае возникновения.

Эта политика охватывает всю организацию и требует неукоснительного соблюдения со стороны всех сотрудников, независимо от их уровня доступа к информационным

ресурсам. Для реализации положений политики информационной безопасности, каждый объект защиты информации закрепляется за конкретным ответственным лицом, назначенным на основании распоряжения руководства организации. Это позволяет обеспечить персональную ответственность за соблюдение мер безопасности и поддержание их на должном уровне [7].

Ключевым аспектом политики является классификация защищаемой информации, которая осуществляется с учетом её значимости и уровня доступа. Эта классификация позволяет присвоить каждому информационному ресурсу соответствующий уровень защиты, что обеспечивает целостность, конфиденциальность и доступность данных в рамках установленной системы информационной безопасности.

В соответствии с рисунком 2 представлена структура концепции ИБ от несанкционированного доступа [8].



Рисунок 2 - Структура концепции ИБ

Концепция информационной безопасности создает прочную систему защиты информации, основываясь на следующих принципах [10]:

- Применение эффективных технических, программных или криптографических средств защиты для нейтрализации

актуальных угроз.

- Увеличение уровня защищенности и минимизация рисков.

- Сохранность информации.

- Создание оптимального комплекса защиты информации и персональных данных в условиях ограниченного бюджета.

- Экономическое обоснование, включая экономию затрат при закупке ПО, лицензий и обновлений.

- Создание условий для продуктивного использования рабочего времени сотрудниками организации.

Концепция информационной безопасности является основой для разработки политики информационной безопасности, которая является единым распорядительным внутренним документом, управляющим комплексными мерами по защите информации и персональных данных в организации.

Для обеспечения многоэшелонированной защиты в организации необходимо разработать организационно-правовые, физические и программные меры обеспечения безопасности.

В соответствии с рисунком 3 представлена схема комплексной системы защиты информации от несанкционированного доступа [12].

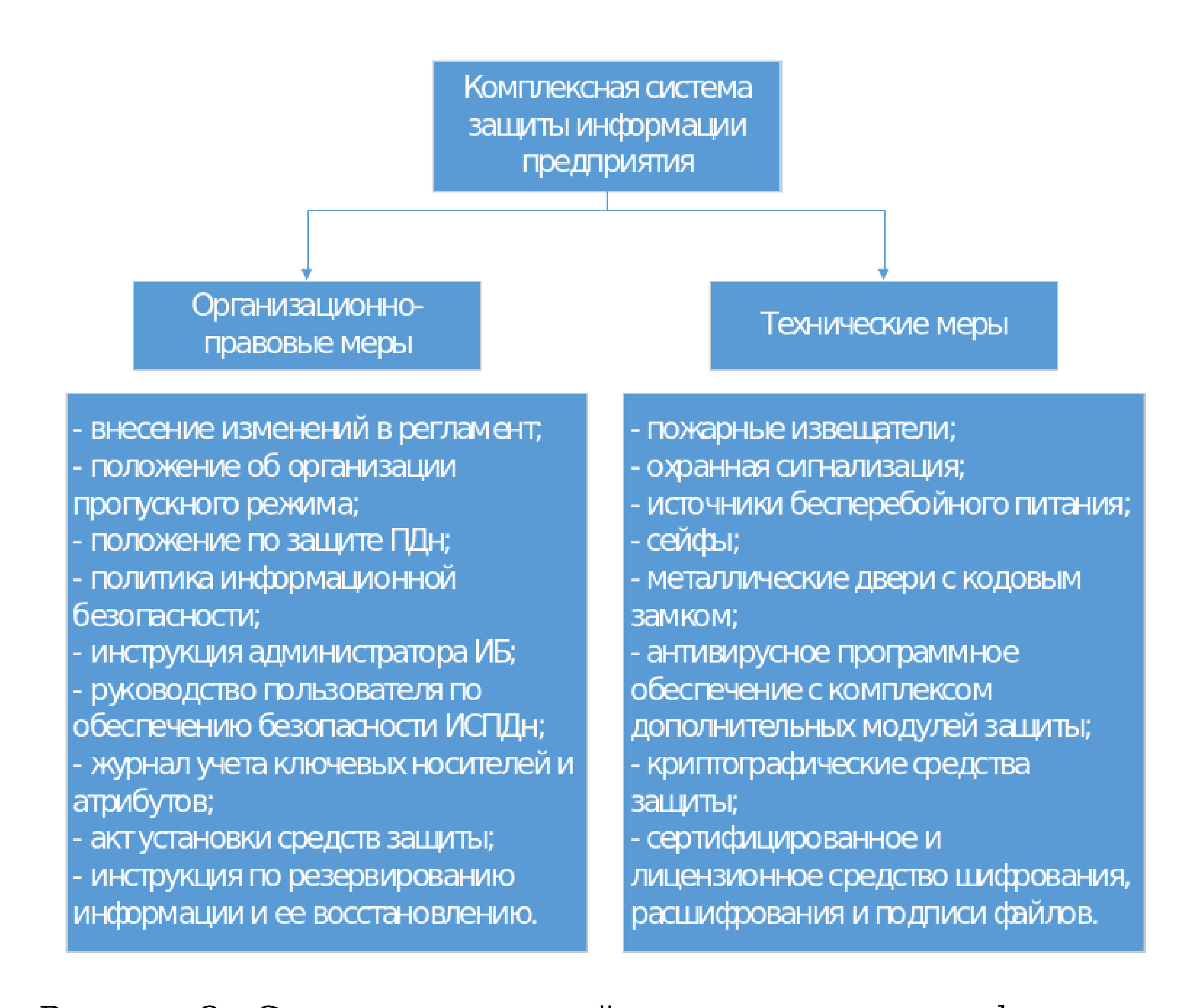


Рисунок 3 - Схема комплексной системы защиты информации

Современная информационная среда подвержена все возрастающему риску несанкционированного доступа и кибератакам. Комплексное обеспечение информационной безопасности становится жизненно важной задачей для защиты ценных данных и ресурсов. В данной работе я обращаю внимание на актуальные угрозы несанкционированного доступа и предлагаю решение для эффективной защиты данных.

Актуальность разработки комплексной системы защиты информации с использованием отечественных средств защиты информации обусловлена несколькими ключевыми факторами. Прежде всего, это национальная безопасность. В условиях геополитической напряженности и санкционного

давления использование решений, не зависящих от иностранных поставок и внешнего влияния, становится критически важным. Отечественные средства защиты информации разрабатываются с учетом специфики национальной инфраструктуры и нормативных требований, что позволяет избежать рисков, связанных с возможными закладками или уязвимостями, которые могут быть использованы иностранными государствами.

Кроме того, российское законодательство, включая федеральный закон № 152-ФЗ «О персональных данных» и согласно указа Президент РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ" [1], требует использования сертифицированных средств защиты информации, которые проверяются на соответствие национальным стандартам и нормативным актам. Отечественные решения часто сертифицированы ФСТЭК и полностью соответствуют необходимым нормативным требованиям, что значительно упрощает их интеграцию и эксплуатацию.

Экономическая целесообразность также играет важную роль. Применение отечественных средств защиты информации поддерживает национальную экономику, способствует созданию рабочих мест и развитию научно-технического потенциала страны. Государственная поддержка таких инициатив позволяет снизить затраты на разработку и внедрение защитных систем благодаря субсидиям и грантам.

Техническая совместимость и адаптация отечественных средств защиты информации к специфике российских

информационных систем обеспечивают их более эффективную интеграцию в существующую инфраструктуру. Такие решения учитывают локальные требования и особенности, что позволяет достичь высокой степени совместимости и надежности.

Использование отечественных решений обеспечивает более высокий уровень доверия со стороны государственных органов и бизнеса. Поскольку исходный код и архитектура таких систем доступны для проверки и аудита национальными регуляторами, это повышает уровень прозрачности и снижает риски, связанные с использованием зарубежных технологий.

Отечественные разработчики могут быстрее реагировать на изменения в законодательстве и требованиях рынка, внося необходимые корректировки в свои продукты и услуги. Это позволяет организациям оперативно адаптироваться к новым условиям и обеспечивать актуальность своих систем защиты информации.

Локальные поставщики также могут обеспечить более высокий уровень поддержки и обслуживания, что особенно важно для критически важных объектов инфраструктуры. Это включает оперативное реагирование на инциденты, регулярные обновления и консультации по вопросам безопасности.

Таким образом, с помощью вышеприведённых схем можно определить набор для комплексной защиты информационной безопасности на любом предприятии. Учитывая уже существующие средства, в результате – можно определить какие еще средства для комплексной защиты информационной безопасности необходимы.

Выводы по главе

Важным аспектом является потребность в обеспечении безопасности данных, что связано с необходимостью сохранения конфиденциальности, целостности и доступности информации. Это особенно актуально в условиях возрастающих киберугроз и сложности современных технологий. Разработка комплексных систем защиты, как показано в работе, предполагает многослойный подход, включающий технические, программные и организационные меры. В главе подчёркнута роль отечественных средств защиты информации в условиях технологической независимости и геополитической напряжённости. Использование таких средств позволяет предприятиям не только соответствовать национальным стандартам, но и минимизировать риски, связанные с уязвимостями и внешними влияниями.

Глава 2. НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И СЕТЕЙ В АО «СИСТЕМНЫЙ ОПЕРАТОР ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ»

2.1. Организационная и финансовая характеристика АО «Системный оператор Единой энергетической системы»

Компания АО «Системный оператор Единой энергетической системы» предоставляет услуги по производству и передаче тепловой энергии от источника тепла к потребителю, гарантируя высококачественное теплоснабжение для клиентов. Наши специалисты осуществляют следующие виды деятельности:

- Мониторинг и контроль за соблюдением оптимальных гидравлических и температурных режимов как для наших собственных источников тепла, так и для ведомственных источников.
- Осуществление проверок на герметичность

тепловых сетей, чтобы гарантировать их бесперебойную работу.

- Проведение ремонтных работ по восстановлению и обслуживанию тепловых сетей, чтобы обеспечивать их эффективную и безопасную работу.

Кроме того, наше предприятие предоставляет услуги сторонним организациям по строительству тепловых сетей с использованием предварительно изолированных труб, а также выполняет гидравлические расчеты и внедряет системы настройки для оптимизации работы тепловых сетей.

В таблице 1 представлены главные показатели филиала компании.

На первых этапах изучения данной предметной области важно ознакомиться с организационной структурой предприятия. Для наглядного представления этой структуры мы можем создать схему, которая показана на рисунке 4. Эта схема представляет собой цельную структуру.

Таблица 1

Главные показатели компании

№ п\п	Наименование характеристики (показателя)	Показатель
1	Протяженность тепловых сетей в 2-х трубном исчислении	278 - пкм
2	Средний диаметр	142 мм
3	Количество котельных	16 ед
4	Годовая выработка тепловой энергии	312 тыс. Гкал
5	Транспорт тепловой энергии	1641 тыс. Гкал
6	Выручка	1,5 млрд. руб.
7	Инвестиционная программа в год	197 млн
8	Объем перекладки тепловых сетей за год	2455 пм
9	Численность персонала	368 человек

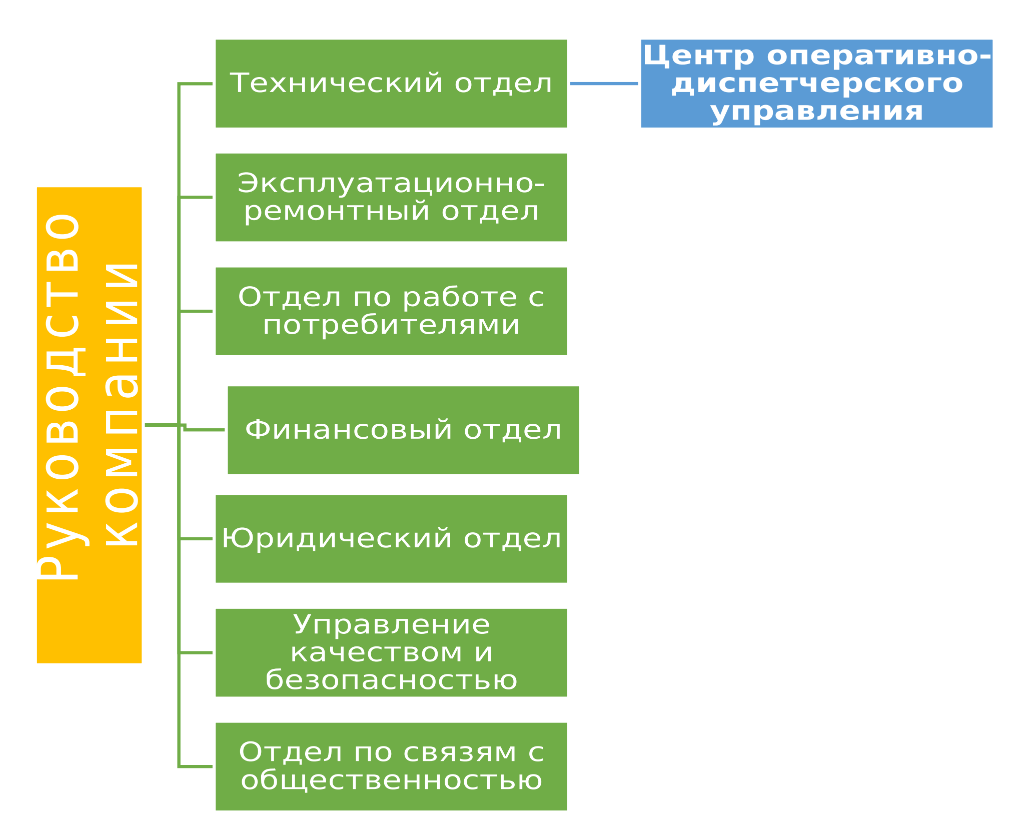


Рисунок 4 - Организационная структура управления предприятием

Организационная структура компании включает в себя следующие элементы:

1. Руководство компании: генеральный директор, заместители, руководители отделов и служб.

2. Технический отдел: инженеры-энергетики, проектировщики, специалисты по оборудованию и технологиям.

3. Эксплуатационно-ремонтный отдел: операторы тепловых сетей, специалисты по обслуживанию и ремонту оборудования.

4. Отдел по работе с потребителями: менеджеры по продажам, специалисты по учету и расчету потребленной тепловой энергии, техническая поддержка и консультации для потребителей.

5. Финансовый отдел: бухгалтерия, финансовый анализ, управление бюджетом.

6. Юридический отдел: специалисты по правовым вопросам, защите прав и интересов компании.

7. Управление качеством и безопасностью: специалисты по контролю за качеством и безопасностью тепловых сетей и оборудования.

8. Отдел по связям с общественностью: специалисты по взаимодействию с государственными и общественными организациями, медиа и потребителями.

Такая организационная структура позволяет компании тепловых сетей эффективно управлять производственными процессами, обеспечивать высокое качество услуг, обеспечивать безопасность и защиту интересов компании, а также удовлетворять потребности потребителей.

В данной работе будет рассмотрен Центр оперативно-диспетчерского управления (ЦОДУ) является важным элементом организационной структуры компании тепловых сетей. ЦОДУ обычно включает в себя команду диспетчеров, которые контролируют работу тепловых сетей и оборудования, управляют режимами работы системы и координируют действия персонала при возникновении аварийных ситуаций.

ЦОДУ должен быть оснащен современными системами мониторинга, управления и автоматического управления тепловыми сетями, которые позволяют оперативно реагировать на изменения в работе системы и устранять возникающие проблемы.

ЦОДУ может быть подчинен как техническому отделу, так и отделу по работе с потребителями, в зависимости от

организационной структуры компании. В любом случае, ЦОДУ является ключевым элементом в обеспечении надежной и безопасной работы тепловых сетей.

Состав и функции Центра представлены на рисунке 5.

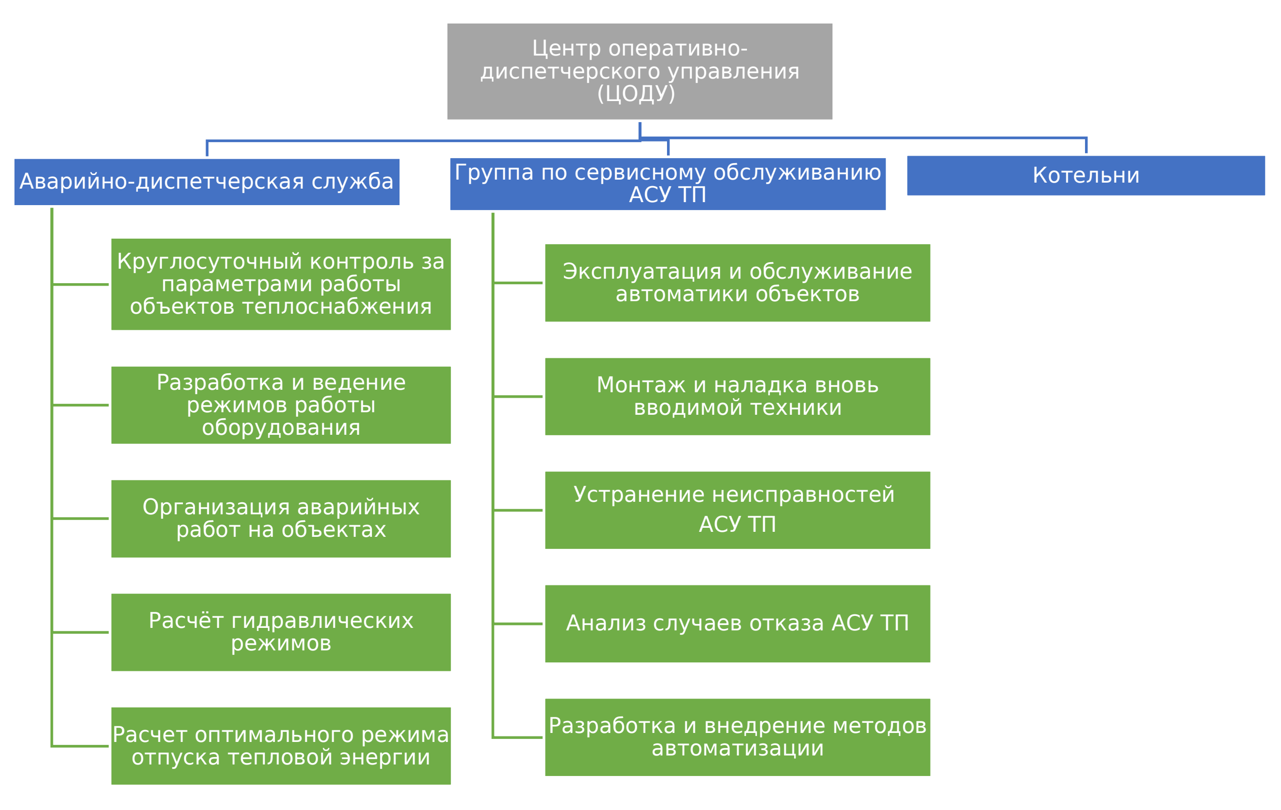


Рисунок 5 - Структура и функции Центра оперативно-диспетчерского управления (ЦОДУ) компании

Центр оперативно-диспетчерского управления (ЦОДУ) включает технический персонал диспетчеров и инженеров.

На рисунке 6 представлена структурная схема технической архитектуры данного предприятия.

Рабочие места обладают следующими характеристиками: процессор Core i3, 8 ГБ оперативной памяти (ОЗУ) и SSD-накопитель емкостью 120 ГБ.

Сервера, используемые на предприятии, включают в себя следующие модели:

- Сервер 1С Intel R1304BTLSHNBR,

- Сервер видеонаблюдения Intel R1304BTLSFANR,
- Сервер виртуальных машин (Mail, АТС Asterisk, Web, AD) Intel R1304BTSSFANR.

В качестве коммутаторов используются следующие модели:

- 3Com 4210/2824 x24,
- D-Link DES 3028P/DGS 3427 x24.

Также в сети присутствует сетевой шлюз D-Link DFL 860E.

Телефонная система состоит из телефонов D-Link DPH-150S.

В качестве периферийных устройств используются следующие модели принтеров:

- HP Color LJ CP4025,
- HP LJ P4014n,
- Xerox WorkCenter 3220,
- Brother HL-5340D.

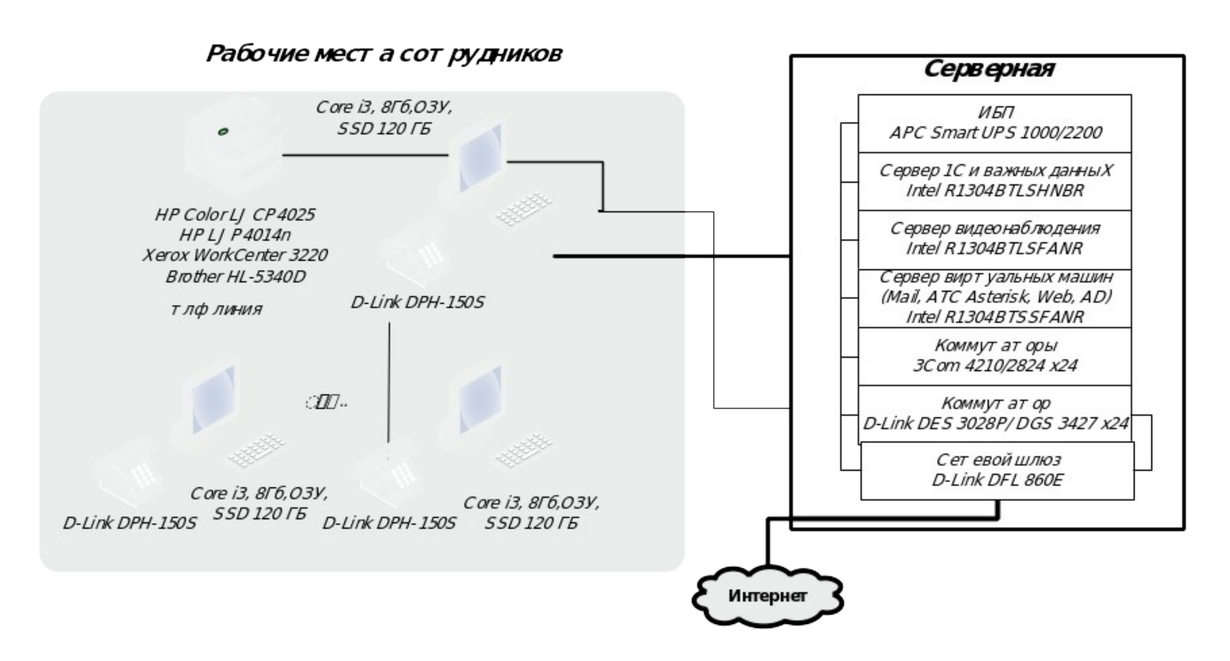


Рисунок 6 - Схема технической архитектуры компании

Техническая архитектура ЦОДУ представлена на рисунке 7. Как видно, связь посредством сети интернет происходит с предприятием и отдаленными котельными с помощью 4G роутера IRZ RL41, в ЦОДУ используется коммутатор Zelax ZES 2028GS, в котельных - Zelax ZES 1208G. Также для хранения и обработки данных о состоянии теплотехнического оборудования в диспетчерской используются серверы базы данных и управляющий сервер.

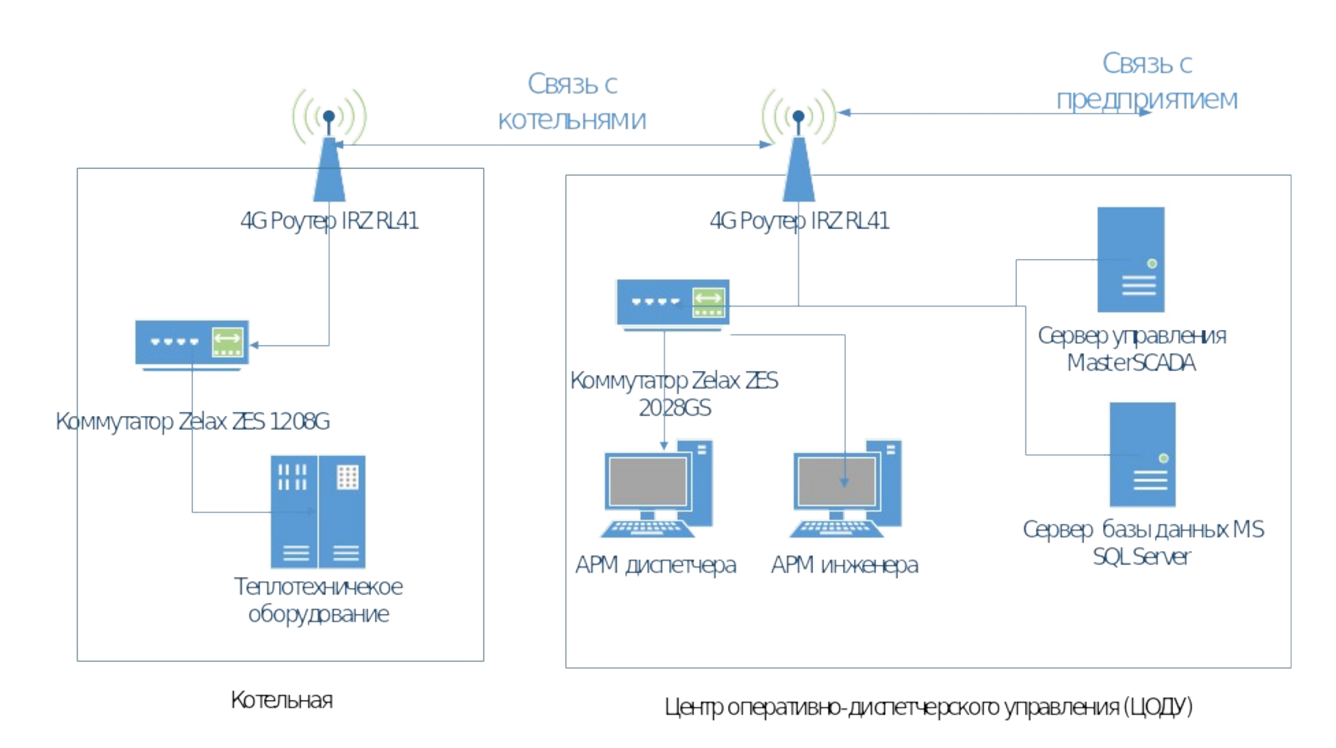


Рисунок 7 - Схема технической архитектуры ЦОДУ

Программная архитектура информационной системы наглядно представлена на рисунке 8.

На всех персональных компьютерах (ПК) предприятия установлен стандартный набор программного обеспечения (ПО), который включает в себя следующие компоненты:

- Операционная система Windows 10 Pro x64;
- Веб-браузер Яндекс. Браузер;
- Офисный пакет Office 2013 "Для дома и бизнеса";

- Антивирусное ПО NOD32;
- Система электронного документооборота (СЭД) IBM Lotus.

Учитывая специфику работы отделов, на всех ПК также установлено дополнительное программное обеспечение (персональные наборы ПО) для соответствующих отделов:

- Отдел СБ (безопасности): Система мониторинга транспорта;
- Бухгалтерия: 1С Бухгалтерия, версия 8.3;
- Центр обработки данных и управления: MasterSCADA;
- Отдел потребителей: ZuluGIS.

На серверах предприятия используются различные операционные системы, включая Windows Server 2016 Standart, CentOS 7 и Ubuntu 16.04.6 LTS. Кроме того, на серверах установлено следующее программное обеспечение:

- FreePBX 12.0.76.2 (система управления телефонной связью);
- Zimbra 8.8.9 (групповая почтовая система);
- SET Remote Administrator (Server), Version 6.5 (6.5.417.0) (удаленное администрирование);
- NOD32 (антивирусное ПО);
- MasterSCADA (система управления и мониторинга);
- Acronis Backup (система резервного копирования);
- 1С Бухгалтерия 8 (бухгалтерская программа).

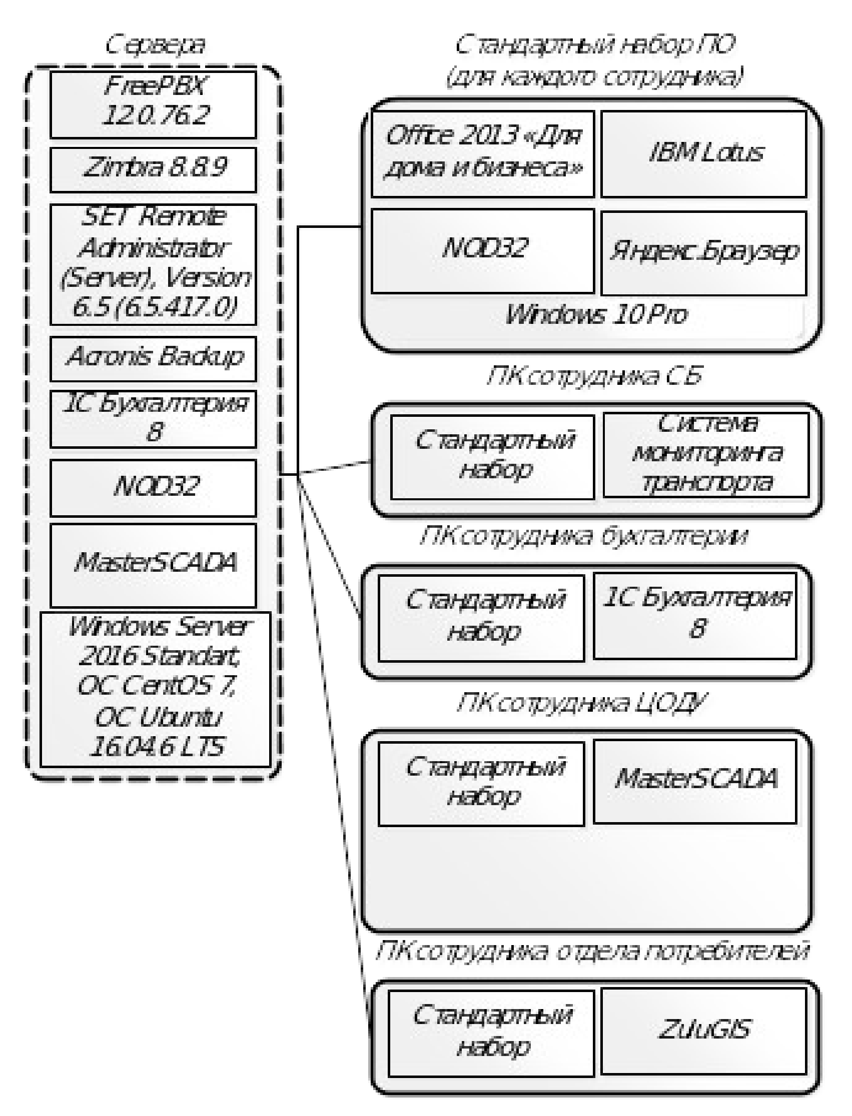


Рисунок 8 - Программная архитектура предприятия

MasterSCADA – программный пакет для создания систем диспетчерского управления и сбора данных. Реализован процесс мониторинга объектов теплоснабжения, а именно контроль параметров:

- Давление теплоносителя.
- Температура теплоносителя.
- Расход теплоносителя.
- Давление холодной воды на источниках тепла.
- Работа насосного оборудования.
- Параметры температуры наружного воздуха, и т.д.

ZuluGIS – геоинформационная система и расчетный комплекс:

- Формирование цифровой карты инженерной сети, объединяющей графическую и семантическую (таблицы характеристик объектов) информацию.
- Создание математической модели системы теплоснабжения.
- Построение пьезометрических графиков, разработка и анализ сценариев перспективного развития тепловых сетей.
- Гидравлический расчет тепловой сети, моделирование режимов работы сети.
- Удаленная работа персонала с данными, размещенными на ZuluServer: поисковые запросы, редактирование информации, передача снимков или документов с мобильного устройства непосредственно на ZuluServer.

Электронный документооборот- СЭД IBM Lotus:

- СЭД представляет из себя целую Экосистему;
- Вся деловая переписка ведется с помощью СЭД (Служебные записки и проч.);
- Приказы, распоряжения по Обществу;
- Инвестпроекты;
- База знаний;
- Договоры;
- Контрагенты;
- Архив Общества.

Система мониторинга транспорта:

- Онлайн мониторинг транспорта;
- Формирование отчетов о простоях и пробегах;
- Исключение случаев хищения топлива и проч.

Помимо этого, на предприятии применяется система контроля и управления доступом, система видеонаблюдения, система охранной сигнализации, пожарной сигнализации.

2.2. Анализ угроз и уязвимостей компании, выявление проблем

Активы предприятия можно разделить на две основные категории: аппаратные ресурсы и информационные ресурсы. Для выделения информационных активов в качестве исходных данных используются следующие параметры:

- Список информации, включающий в себя ведомственные, государственные и коммерческие секреты.
- Перечень источников информации на предприятии.

Структурирование информации осуществляется путем классификации по структуре, функциям и задачам предприятия, с указанием источников, где эта информация хранится.

Конфиденциальной информацией считаются следующие виды данных:

- Информация о деятельности предприятия.
- Данные о клиентах предприятия.
- Служебная информация о финансовом положении предприятия.
- Сведения о системе безопасности предприятия.
- Записи и документация, содержащие информацию о переговорах с клиентами.

В таблице 2 представлен список активов, которые требуют дополнительной защиты и контроля.

Таблица 2

Оценка информационных активов предприятия

Вид деятельности	Наименование актива	Форма предоставле-ния актива	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Кол.оцен-ка (руб.)	Кач. оценка
Руководство компании	Уставы и юридические дела	Бумажный документ, Электронный документ на ЖМД, Персонал	Генеральный директор, заместители, руководители отделов и служб	Финансовый успех, репутация	80000	Критичное
Технический отдел	Технические чертежи и документация	Электронный документ на ЖМД, Персонал	Инженеры - энергетики, проектировщики, специалисты по оборудованию и технологиям	Критическая информация, технические данные	75000	Высокое
Эксплуатационно-ремонтный отдел	Технические схемы и обслуживание	Электронный документ на ЖМД, Персонал	Операторы тепловых сетей, специалисты по обслуживанию и ремонту оборудования	Критическая информация, обслуживание оборудования	60000	Высокое

Вид деятельности	Наименование актива	Форма предоставле-ния актива	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Кол.оцен-ка (руб.)	Кач. оценка
Отдел по работе с потребителями	Данные о потреблении и контактах	Электронный документ на ЖМД, Персонал	Менеджеры по продажам, специалисты по учету и расчету потребленной тепловой энергии, техническая поддержка и консультации для потребителей	Клиентская информация	70000	Высокое
Финансовый отдел	Финансовые отчеты и бюджет	Электронный документ на ЖМД, Персонал	Бухгалтерия, финансовый анализ, управление бюджетом	Финансовые данные	85000	Критичное

Продолжение таблицы 2

Вид деятельности	Наименование актива	Форма предоставле-ния актива	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Кол.оцен-ка (руб.)	Кач. оценка
Юридический отдел	Договоры и правовая документация	Бумажный документ, Электронный документ на ЖМД, Персонал	Специалисты по правовым вопросам, защите прав и интересов компании	Критическая информация, юридическая документация	75000	Критичное
Управление качеством и безопасностью	Данные о проверках и аудитах	Электронный документ на ЖМД, Персонал	Специалисты по контролю за качеством и безопасностью тепловых сетей и оборудования	Контрольные данные	70000	Высокое
Отдел по связям с общественностью	Коммуникационные материалы и отчеты	Электронный документ на ЖМД, Персонал	Специалисты по взаимодействию с государственными и общественными организациями, медиа и потребителями	Коммуникационные данные	60000	Высокое
Центр оперативно-диспетчерского управления (ЦОДУ)	Данные о работе и управлении сетями	Электронный документ на ЖМД, Персонал	Специалисты ЦОДУ	Контрольные данные, данные о работе и управлении сетями	90000	Критичное

В таблице 3 приведены активы, обладающие наибольшей ценностью и по этой причине избранные как объект защиты информации.

Таблица 3

Итоги ранжирования активов компании

Наименование актива	Ценность актива (ранг)
Уставы и юридические дела предприятия	5
Технические чертежи и документация	5
Технические схемы и обслуживание	5
Данные о потреблении и контактах	4
Финансовые отчеты и бюджет	3
Договоры и правовая документация	3
Данные о работе и управлении сетями	3

Уязвимости информационных активов представляют собой недостатки, которые могут привести к нежелательным последствиям, таким как воздействие со стороны вредоносного кода, неопытных сотрудников или злоумышленников [25]. Для выявления уязвимостей в информационной системе предприятия существует несколько методов, которые могут описать сотрудники компании, исходя из своего опыта. Кроме того, можно пригласить внешних экспертов для проведения технологической аудитории информационной системы и обнаружения всех уязвимостей.

На нашем анализируемом предприятии уязвимости активов оцениваются согласно ГОСТ Р ИСО/МЭК ТО 13335-3-2007 "Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий" с использованием общего подхода. В ходе этой оценки учитываются следующие критерии для определения ущерба от потери целостности, конфиденциальности или доступности активов [11]:

- Снижение эффективности бизнеса.
- Нарушение законодательства или подзаконных актов.

- Утрата престижа предприятия.
- Нарушение персональной безопасности.
- Нарушение безопасности личных данных.
- Негативное воздействие на соблюдение законности.
- Нарушение общественного порядка.
- Нарушение конфиденциальности коммерческой информации.
- Финансовые потери.
- Нарушение бизнес-сделок.
- Угроза окружающей среде.

Результаты оценки уязвимостей представляются в виде списка, в котором для каждой уязвимости указываются оценка риска информационной безопасности, стоимость актива и вероятность реализации угрозы. Эти результаты можно увидеть в Таблице 4.

Таблица 4

Итоги оценки уязвимости активов предприятия

Группа уязвимостей	Содержание уязвимости	Финансовые отчеты предприятия	Персональные данные работников	Система обеспечения безопасности предприятия	Сведения о схемах размещения систем безопасности	Маркетинговые исследования рынка	Внутренняя бухгалтерская документация	Сведения о достигнутых договоренностях и соглашениях	Сведения о PR-компаниях
Физическая безопасность	Недостаточная защита оборудования	Средняя	Низкая	Низкая	Высокая	Низкая	Низкая	Низкая	Низкая
Информационная безопасность	Недостаточная защита данных	Средняя	Низкая	Средняя	Высокая	Низкая	Низкая	Высокая	Низкая
Финан	Неправи	Высо	Низк	Низк	Сред	Низка	Высо	Низка	Низ

совая безопасность	льное ведение бухгалтерии	кая	ая	ая	няя	я	кая	я	кая
Клиентские данные	Несанкционированный доступ	Низкая	Средняя	Средняя	Низкая	Средняя	Низкая	Высокая	Низкая
Репутационная безопасность	Утечка информации о PR-компаниях	Низкая	Низкая	Низкая	Низкая	Высокая	Низкая	Низкая	Средняя

Выводы из этой таблицы следующие:

- уровень уязвимости для оборудования на тепловых станциях оценивается как средний, что означает, что необходимы дополнительные меры безопасности для защиты физической инфраструктуры.
- уязвимость в отношении данных о схемах размещения систем безопасности оценивается как высокая, что подчеркивает необходимость усиления защиты информационных активов.
- проблемы с ведением бухгалтерской документации оцениваются как высокие, что может представлять серьезный риск для финансовой стабильности компании.
- уровень уязвимости от несанкционированного доступа к данным клиентов оценивается как средний, что требует более тщательных мер для обеспечения безопасности клиентской информации.
- утечка информации о PR-компаниях оценивается как высокая уязвимость, что может повредить репутацию компании и требует активных мер для защиты репутации.

Выводы из этой таблицы подчеркивают необходимость улучшения безопасности компании в различных аспектах ее

деятельности.

В таблице 5 показана вероятность реализации угрозы для конкретного актива информационного ресурса.

Таблица 5

Итоги оценки угроз активам предприятия

Группа угроз	Содержание угроз	Уставы и юридические дела	Технические чертежи и документация	Технические схемы и обслуживание	Данные о потреблении и контактах	Финансовые отчеты и бюджет	Договоры и правовая документация	Данные о проверках и аудитах	Коммуникационные материалы и отчеты	Данные о работе и управлении сетями
Внутренние угрозы	Несанкционированный доступ сотрудников	Высокая	Средняя	Низкая	Средняя	Низкая	Высокая	Средняя	Низкая	Средняя

Продолжение таблицы 5

Группа угроз	Содержание угроз	Уставы и юридические дела	Технические чертежи и документация	Технические схемы и обслуживание	Данные о потреблении и	Финансовые отчеты и бюджет	Договоры и правовая документация	Данные о проверках и аудитах	Коммуникационные материалы и отчеты	Данные о работе и управлении сетями
Внешние угрозы	Кибератаки на информационную инфраструктуру, направленные на нарушение работы системы управления сетями и передачи тепловой энергии.	Низкая	Средняя	Высокая	Низкая	Высокая	Низкая	Низкая	Средняя	Низкая
Физические угрозы	Пожары или наводнения, которые могут повредить технические схемы и обслуживание.	Низкая	Высокая	Низкая	Средняя	Средняя	Низкая	Низкая	Низкая	Низкая
Угрозы связанные с клиентами	Отказ клиентов от услуг из-за неудовлетворительного качества теплоснабжения.	Средняя	Низкая	Низкая	Низкая	Высокая	Высокая	Низкая	Средняя	Низкая
Репутационные угрозы	Утечка информации о несоблюдении норм экологической безопасности, что может негативно сказаться на репутации компании.	Низкая	Средняя	Низкая	Низкая	Низкая	Низкая	Низкая	Низкая	Средняя
Угрозы инфор	Вирусы и вредоносные программы,	Средняя	Низкая	Низкая	Низкая	Средняя	Низкая	Низкая	Низкая	Средняя

мацио нной безоп аснос ти	которые могут атаковать информационн ую инфраструктур у и воровать конфиденциал ьные данные.									

Продолжение таблицы 5

Группа угроз	Содержание угроз	Уставы и юридические дела	Технические чертежи и документация	Технические схемы и обслуживание	Данные о потреблении и	Финансовые отчеты и бюджет	Договоры и правовая документация	Данные о проверках и аудитах	Коммуникационные материалы и отчеты	Данные о работе и управлении сетями
Угрозы финансовой безопасности	Мошенничество или взлом с целью получения доступа к финансовым отчетам и бюджету.	Высокая	Низкая	Низкая	Средняя	Низкая	Средняя	Низкая	Низкая	Низкая
Юридические угрозы	Правовые действия со стороны регулирующих органов в случае нарушения законодательства в сфере энергетики.	Средняя	Низкая	Низкая	Низкая	Низкая	Низкая	Высокая	Низкая	Низкая

Результаты анализа, проведенного в отношении программных и аппаратных средств, используемых для обеспечения информационной безопасности предприятия, отражены в таблице 6 [1]. Эта таблица представляет оценку выполнения основных задач, связанных с обеспечением информационной безопасности в организации.

Таблица 6

Анализ выполнения ключевых задач, связанных с обеспечением информационной безопасности предприятия.

Задачи обеспечения ИБ	Уровень выполнения, %
Обеспечение безопасности информационных процессов и документооборота	54
Защита информации в информационных системах	45

Обеспечение конфиденциальности переговоров и коммуникаций	43
Обеспечение безопасности взаимодействия с партнерами и клиентами	66
Сохранение конфиденциальности персональных данных сотрудников и клиентов	23
Сохранение коммерческой тайны	56

Из представленных данных видно, что ни одна из задач, связанных с обеспечением информационной безопасности в предприятии, не выполняется полностью.

Внедрение системы межсетевого экранирования на предприятии представляет собой ключевую меру повышения уровня информационной безопасности, поскольку она позволяет обеспечить защиту от несанкционированного доступа, вредоносных воздействий и утечки конфиденциальных данных, а также способствует фильтрации сетевого трафика и контролю доступа сотрудников к внешним ресурсам. Такая система обеспечивает стабильную и непрерывную работу корпоративной сети, снижает вероятность успешных атак и позволяет организовать безопасное подключение удалённых пользователей через VPN. Кроме того, межсетевое экранирование поддерживает выполнение требований отраслевых нормативов по защите информации, способствует сокращению финансовых потерь от киберинцидентов и повышает доверие со стороны партнёров и клиентов [15].

На данном предприятии обеспечение защиты автоматизированных систем сопровождается регулярной оценкой рисков информационной безопасности в соответствии с положениями ГОСТ Р ИСО/МЭК ТО 27005-3-2010. Основу оценки составляет качественный подход, при котором уровень риска определяется по совокупности вероятности реализации угроз и тяжести последствий,

возникающих при утрате свойств конфиденциальности, целостности и доступности информации. В рамках оценки проводится идентификация информационных активов, объектов среды, источников угроз и степени их воздействия, что позволяет формировать обоснованные управленческие решения по усилению защищённости корпоративной инфраструктуры [13].

Результаты оценки рисков представляются в виде списка рисков, каждому из которых присваивается ранг по пятибалльной шкале. Данные оценки рисков представлены в Таблице 7.

Таблица 7

Итоги оценки рисков информационным активам предприятия [7]

Риск	Актив	Ранг риска
Превышение допустимой нагрузки	Финансовые отчеты и бюджет	3
	Данные о проверках и аудитах	3
	Данные о работе и управлении сетями	3
Сбои и отказы программных средств	Внутренняя бухгалтерская документация	3
	Данные о достигнутых соглашениях и договоренностях	3
	Коммуникационные материалы и отчеты	3
	Финансовые отчеты и бюджет	3
Недобросовестное исполнение обязанностей	Данные о работе и управлении сетями	3
	Система обеспечения безопасности предприятия	3
	Технические чертежи и документация	3
Выполнение вредоносных программ	Внутренняя бухгалтерская документация	3
	Данные о достигнутых соглашениях и договоренностях	3
Использование информационных активов не по назначению	Коммуникационные материалы и отчеты	2
	Финансовые отчеты и бюджет	2
	Технические чертежи и документация	2
	Система обеспечения безопасности предприятия	2
Нарушения персоналом организационных мер по обеспечению ИБ	Технические схемы и обслуживание	2
	Данные о проверках и аудитах	2
	Данные о достигнутых соглашениях и договоренностях	2
Действия неавторизованного субъекта	Коммуникационные материалы и отчеты	2
	Финансовые отчеты и бюджет	2
Неконтролируемая модификация информационного актива	Система обеспечения безопасности предприятия	1
	Технические схемы и обслуживание	1
Несанкционированный доступ	Внутренняя бухгалтерская документация	1
	Данные о достигнутых соглашениях и договоренностях	1
	Коммуникационные материалы и отчеты	1

Из таблицы 8 можно выявить, какие виды деятельности связаны с обеспечением безопасности информации и на какие органы или должности возлагается ответственность за эти виды деятельности [14].

Таблица 8

Информационная безопасность предприятия [13]

Виды операций	Информационные ресурсы		
	Бумажные документы	Электронные документы	Информация и знания работников
Создание информационного ресурса (создание и оформление документов)	Финансовый отдел, технический отдел	Финансовый отдел, технический отдел	Финансовый отдел, технический отдел
Оперативная работа с документами и документационное обеспечение деловых процессов	Эксплуатационно-ремонтный отдел	Эксплуатационно-ремонтный отдел	Не регламентируется
Организация документооборота	Финансовый отдел	Руководство компании, юридический отдел	Отдел по работе с потребителями
Обеспечение соответствия требованиям законодательства	Руководство компании, отдел по связям с общественностью	Отдел по работе с потребителями	Руководство компании
Учет документов (ознакомленности с информацией)	Финансовый отдел	Отдел по работе с потребителями	Не регламентируется
Уничтожение документов по установленным правилам, с оформлением акта	Финансовый отдел	Отдел по работе с потребителями	Отдел по работе с потребителями
Резервирование документов и информации	Юридический отдел	Отдел по работе с потребителями	Отдел по работе с потребителями
Управление доступом	Руководство компании, юридический отдел	Руководство компании, юридический отдел	Руководство компании
Физическая защита (обеспечение наличия ресурса)	Руководство компании, юридический отдел	Руководство компании, юридический отдел	Руководство компании, юридический отдел
Защита важнейших документов	Руководство компании	Руководство компании	Руководство компании
Защита конфиденциальной	Руководство компании,	Руководство компании,	Руководство компании

Виды операций	Информационные ресурсы		
	Бумажные документы	Электронные документы	Информация и знания работников
информации и персональных данных	юридический отдел	юридический отдел	

Также из таблицы видно, что практически все нерешенные проблемы в области обеспечения информационной безопасности возникают из-за того, что ни одна из служб не сотрудничает со всеми информационными ресурсами, а ограничивается работой только с одним из них. Другими словами, в таких случаях деятельность по обеспечению информационной безопасности считается нескоординированной.

В свете данных обстоятельств и увеличивающихся требований к информационной безопасности со стороны государственных органов было принято решение разработать документ, который бы строго регламентировал порядок действий, объем обязанностей и полномочий всех сотрудников, ответственных за обеспечение информационной безопасности предприятия. В таком документе, как правило, содержится "Политика безопасности предприятия" [19].

Основная цель политики информационной безопасности заключается в установлении общих правил и норм взаимодействия с информацией на предприятии. Утвержденные и документированные правила по обеспечению информационной безопасности обеспечивают следующие цели [18]:

- Обеспечение независимости защиты от профессиональных и личных характеристик сотрудников.
- Обеспечение стабильности уровня защиты.

- Позволяет осуществлять контроль над процессами обеспечения безопасности и обработки информации.

Перед тем как приступить к разработке политики информационной безопасности (ИБ), необходимо провести анализ активов. Этот анализ включает в себя учет и оценку активов компании. Завершенная политика ИБ должна включать специальный раздел для каждого обнаруженного актива, а также для групп связанных активов или отдельных компонентов активов, в зависимости от ранее проведенного анализа их структуры и взаимосвязей.

Сформулированная политика информационной безопасности предприятия должна быть доступной для понимания всеми сотрудниками, с акцентом на практическую применимость и минимизацию специальной терминологии. Одним из её ключевых компонентов выступает сетевая политика, регулирующая принципы взаимодействия с сетевой инфраструктурой и задающая правила обработки, контроля и защиты сетевого трафика. Эта политика включает как общие положения, так и конкретные конфигурации систем защиты информации, таких как межсетевые экраны, средства обнаружения атак и криптографические шлюзы.

Политики безопасности конкретных систем, например, межсетевого экрана, фиксируют способы обработки трафика, механизмы обновления и управления. Они реализуются через конфигурации, которые могут задаваться с помощью командной строки или графических интерфейсов. Каждое правило в таких системах представляет собой реализацию положений общей политики безопасности, и все элементы должны быть логически согласованы между собой.

Политики должны быть логичны, однозначны,

документированы и регулярно обновляться, чтобы отражать текущие угрозы. Их содержание должно соответствовать целям защиты данных, быть прозрачным для участников информационного обмена и обеспечивать минимальные препятствия в работе персонала. Реализация политики затрагивает широкий круг направлений: от организационных и технических до юридических, включая подготовку внутренней документации, соблюдение правовых норм и создание инженерно-технической инфраструктуры защиты.

Практическая реализация политики безопасности требует разделения обязанностей и наличия специализированного персонала. Ответственность за техническую защиту несёт соответствующее подразделение, которое занимается выявлением каналов утечки, организацией контроля и разработкой защитных мероприятий. При этом сотрудники обязаны соблюдать установленные процедуры: ограничение доступа, контроль за ключами и паролями, регламентированное обращение с документами, а также использование сетевых ресурсов строго по рабочим задачам.

Все требования политики должны быть адаптированы к текущей обстановке, не нарушать производственные процессы и учитывать актуальные уязвимости. В дипломной работе планируется провести анализ организационных и инженерных аспектов реализации политики, определить комплекс необходимых мер и средств обеспечения информационной безопасности, а также рассчитать экономическую целесообразность проекта.

Более подробные требования обычно применяются в политиках на более низком уровне управления и отладки

системы защиты информации, таких как межсетевой экран, системы обнаружения и предотвращения вторжений, контроля утечек данных, криптографические шлюзы, коммутаторы и маршрутизаторы. Давайте, для примера, рассмотрим политику информационной безопасности, касающуюся межсетевого экрана (МЭ).

Политика МЭ существенно отличается от политики ИБ на более высоких уровнях, поскольку она представляет собой описание того, как будет осуществляться работа МЭ и связанных с ним механизмов безопасности. Эта политика определяет, как МЭ будет обрабатывать сетевой трафик, а также как он будет обновляться и управляться.

Почти все МЭ используют правила как механизм управления безопасностью. Смысл этих правил определяет фактическую функциональность МЭ, и количество данных в правилах может различаться в зависимости от архитектуры МЭ.

Для управления такой конфигурацией МЭ обычно применяют один из двух механизмов. Первый - это интерфейс командной строки, который позволяет администратору настраивать МЭ с помощью ввода команд. Этот метод может быть подвержен ошибкам, связанным с неправильным вводом команды, но опытные администраторы могут настраивать МЭ и быстро реагировать на нештатные ситуации.

Второй метод - настройка МЭ через графический интерфейс, который более прост в использовании и позволяет администратору настраивать сложные системы быстрее. Однако графический интерфейс может быть менее подробным, и некоторые настройки, доступные через командную строку, могут быть недоступны в графическом

интерфейсе. В таких случаях администратору приходится воспользоваться командной строкой для настройки конфигурации.

В конечном итоге, правила сетевой политики информационной безопасности создаются как часть конфигурации определенной СЗИ. Под конфигурацией понимается совокупность параметров СЗИ, определяющая ее работу.

С учетом указанных выше требований и особенностей политик для СЗИ, можно заключить, что различные виды политик и другие правила, заданные в СЗИ, взаимосвязаны между собой. Сетевая политика информационной безопасности соответствует политике информационной безопасности компании и полностью согласуется с ней. В свою очередь, политика конкретного СЗИ дополняет сетевую политику информационной безопасности и выражает ее положения для конкретной системы безопасности. Все правила, установленные в СЗИ, по сути, представляют собой реализацию высокоуровневой политики на практике. Следовательно, для эффективного управления информационной безопасностью необходимо включать политики всех уровней.

2.3. Предложения с экономическим обоснованием по совершенствованию информационной безопасности автоматизированных систем и сетей в АО «Системный оператор Единой энергетической системы»

2.3.1. Анализ существующих систем

При таких ограничениях и запретах на использование

иностранного программного обеспечения на значимых объектах критической информационной инфраструктуры России согласно указа Президент РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ" [1], важным становится использование отечественных решений, в том числе систем межсетевого экранирования (МСЭ).

Для энергетических компаний, важных объектов критической информационной инфраструктуры, будет целесообразным рассмотрение отечественных МСЭ-решений, таких как UserGate, Континент 4, xFirewall 5, Ideco UTM, Dionis DPS, Diamond VPN/FW. При выборе системы следует учитывать не только технические характеристики, но и соответствие стандартам безопасности и сертификациям, а также обновления и поддержку отечественных поставщиков.

Такие меры направлены на обеспечение технологической независимости и повышение кибербезопасности стратегически важных объектов.

Для анализа отечественных систем межсетевого экранирования выбраны следующие системы российского производства:

- Usergate;
- Ideco UTM;
- Континент 4;
- xFirewall 5;
- Dionis DPS;
- Diamond VPN/FW.

В таблице 9 представлено сравнение систем межсетевого экранирования по критерию «Производительность».

На основании анализа сравнительной таблицы можно обобщить, что решения Dionis DPS и xFirewall 5 демонстрируют наивысшие показатели производительности как в режиме базовой фильтрации трафика, так и при включении дополнительных функций, включая поддержку большого числа одновременных сессий. UserGate, Ideco UTM и Diamond VPN/FW также характеризуются высокой скоростью обработки трафика и масштабируемостью, позволяя эффективно функционировать в сетях различной сложности. Особенно выделяются Dionis DPS и UserGate по количеству поддерживаемых интерфейсов, что предоставляет им дополнительные преимущества при построении отказоустойчивых решений.

Таблица 9

Сравнение систем межсетевого экранирования по критерию «Производительность»

Критерий производительности	UserGate	Ideco UTM	Континент 4	xFirewall 5	Dionis DPS	Diamond VPN/FW
Скорость Firewall (Гбит/с)	До 60	До 76,3	До 80	До 19	До 90	До 48
Производительность с включенными функциями (Гбит/с)	До 8	До 3,7	До 7	До 669 Мбит/с	До 8	До 8
Максимальное количество сессий	48 000 000	5 000 000	10 000 000	9 900 000	60 000 000	10 000 000
Максимальное количество портов Ethernet 10/100/1000	До 49	До 9	До 6	До 6	До 32	До 48
Максимально	До 24	До 8	До 4	До 4	До 48	До 24

Критерий производительности	UserGate	Ideco UTM	Континент 4	xFirewall 5	Dionis DPS	Diamond VPN/FW
е количество портов SFP+						10G SFP+, До 12 40GbE QSFP+
Поддержка нескольких провайдеров	Да	Да	Да	Да	Да	Да
Аппаратное ускорение	В разработке	Возможность установки криптоускорителя	Отсутствует	Отсутствует	Отсутствует	Отсутствует
Сертификация ФСТЭК России	Есть	Есть	Есть	Есть	Есть	Есть
Сертификация ФСБ России	Отсутствует	Планируется получение	Отсутствует	Отсутствует	Отсутствует	Есть
Сертификация российской радиоэлектронной продукции	Включён аппаратный комплекс UserGate C150	В реестре ТОРП	Не включён в реестр	Отсутствует	Отсутствует	Отсутствует

Все рассматриваемые решения поддерживают работу с несколькими провайдерами, что обеспечивает гибкость маршрутизации и отказоустойчивость. У некоторых систем предусмотрена возможность использования аппаратных криптоускорителей, что может значительно повысить эффективность при шифровании VPN-трафика. С точки зрения соответствия нормативным требованиям, наибольшее число сертификаций у Dionis DPS и xFirewall 5, что делает их предпочтительными в критически важных информационных инфраструктурах. При этом аппаратные решения UserGate внесены в реестр российской радиоэлектронной продукции, что актуально для предприятий, придерживающихся

политики импортозамещения и соответствия требованиям законодательства РФ.

В таблице 10 представлено сравнение систем межсетевого экранирования по критерию «Функциональность».

Таблица 10

Сравнение систем межсетевого экранирования по критерию «Функциональность»

Критерии	UserGate	Ideco UTM	Континент 4	xFirewall 5	Dionis DPS	Diamond VPN/FW
Управление	Централизованное, роли	Централизованное, роли	Централизованное, роли	Централизованное, роли	Централизованное	Ограниченные встроенные роли
Безопасность	Межсетевой экран, СОВ, 2ФА	Межсетевой экран, СОВ, 2ФА	Межсетевой экран, СОВ	Межсетевой экран, СОВ	Межсетевой экран, СОВ	Межсетевой экран, 2ФА
Логирование	Подробный журнал, логи действий	Журнал событий, SNMP	Журнал событий, SNMP, оповещения	Журналы, SIEM, оповещения	Журналы, SNMP	Журнал событий, различные журналы
Производительность	Высокая, много сессий	Высокая, SNMP	Высокая, балансировка, VLAN	Высокая, балансировка, VLAN	Очень высокая, много портов	Высокая, VLAN, балансировка

Анализируя сравнительную таблицу, можно отметить, что большинство решений, включая UserGate, Ideco UTM, Континент 4 и xFirewall 5, предлагают развитую систему централизованного управления с разграничением административных ролей, что облегчает эксплуатацию и контроль. Diamond VPN/FW в этом аспекте несколько уступает из-за ограниченности встроенных ролей.

С точки зрения обеспечения безопасности, все решения реализуют базовые механизмы защиты, включая межсетевой экран и системы обнаружения вторжений, а также — в некоторых случаях — поддержку двухфакторной аутентификации, как это реализовано в UserGate, Ideco UTM и Diamond VPN/FW. Это позволяет значительно повысить надёжность аутентификации и доступ к критическим ресурсам.

Функциональность в области логирования и мониторинга представлена разнообразно: UserGate и Ideco UTM обеспечивают полный журнал событий и развитую систему мониторинга, Континент 4 и xFirewall 5 поддерживают сетевые протоколы мониторинга и уведомления, а Dionis DPS демонстрирует высокий уровень интеграции с системами анализа безопасности за счёт поддержки SNMP и SIEM. Diamond VPN/FW также позволяет отслеживать события через встроенные механизмы журналирования.

Что касается производительности, все представленные решения демонстрируют высокий уровень пропускной способности и поддержку большого количества сессий. Особенно выделяются Dionis DPS, xFirewall 5 и Континент 4 благодаря наличию широких возможностей по балансировке нагрузки и поддержке VLAN, что делает их особенно подходящими для комплексных сетевых инфраструктур.

В таблице 11 представлено сравнение систем межсетевого экранирования по критерию «Масштабируемость».

Таблица 11

Сравнение систем межсетевого экранирования по критерию «Масштабируемость»

Система	Масштабируемость
UserGate	До 60 Гбит/с; до 8 Гбит/с с включенными функциями
Ideco UTM	До 76,3 Гбит/с; до 3,7 Гбит/с с включенными функциями
Континент 4	До 7 Гбит/с; до 5 млн. максимальных сессий
xFirewall 5	До 669 Мбит/с
Dionis DPS	До 8 Гбит/с; до 60 млн. максимальных сессий
Diamond VPN/FW	До 8 Гбит/с; до 10 млн. максимальных сессий

Обобщая результаты сравнительного анализа, можно отметить, что Dionis DPS отличается высокой масштабируемостью за счёт поддержки значительного количества одновременных сессий, что делает её эффективной для крупных сетевых инфраструктур. UserGate и Ideco UTM демонстрируют высокую пропускную способность при сохранении стабильной работы при больших нагрузках, сочетая производительность с гибкостью настройки. Континент 4 и Diamond VPN/FW также показывают удовлетворительную масштабируемость, соответствующую их техническим параметрам, что позволяет эффективно использовать их в средних по объёму сетях.

В таблице 12 представлено сравнение систем межсетевого экранирования по критерию «Совместимость».

Таблица 12

Сравнение систем межсетевого экранирования по критерию «Совместимость»

Система	Совместимость
UserGate	Поддерживает Vmware, Hyper-V, VirtualBox, KVM, XenServer, OpenStack, Citrix, Oracle VM Server
Ideco UTM	Поддерживает Vmware, Hyper-V, VirtualBox, KVM, XenServer, OpenStack, Citrix, Oracle VM Server
Континент 4	Поддерживает Vmware, Hyper-V, VirtualBox, не гарантируется для KVM, XenServer, OpenStack, Citrix, Oracle VM Server
xFirewall 5	Поддерживает Vmware, Hyper-V, VirtualBox, KVM, не

	гарантируется для XenServer, OpenStack, Citrix, Oracle VM Server
Dionis DPS	Поддерживает Vmware, Hyper-V, VirtualBox, не гарантируется для KVM, XenServer, OpenStack, не гарантируется для Citrix, не гарантируется для Oracle VM Server
Diamond VPN/FW	Поддерживает Vmware, не гарантируется для Hyper-V, VirtualBox, KVM, XenServer, OpenStack, не гарантируется для Citrix, не гарантируется для Oracle VM Server

Из анализа совместимости с виртуализационными средами следует, что UserGate и Ideco UTM демонстрируют наибольшую универсальность, обеспечивая стабильную работу на широком спектре виртуализационных платформ. Континент 4 и xFirewall 5 также поддерживают основные решения виртуализации, однако в их использовании возможны отдельные ограничения, влияющие на гибкость развертывания. В то же время Dionis DPS и Diamond VPN/FW демонстрируют ограниченную совместимость, что сужает возможности их интеграции в виртуализованные ИТ-инфраструктуры.

В таблице 13 представлено сравнение систем межсетевого экранирования по критерию «Безопасность».

Таблица 13

Сравнение систем межсетевого экранирования по критерию «Безопасность»

Система	Безопасность
UserGate	Сертификация ФСТЭК России, отсутствие сертификата ФСБ, включение в реестр радиоэлектронной продукции, запись в реестр российских программ для ЭВМ и баз данных
Ideco UTM	Сертификация ФСТЭК России, отсутствие сертификата ФСБ, запись в реестр российских программ для ЭВМ и баз данных
Континент 4	Сертификация ФСТЭК России, отсутствие сертификата ФСБ, включение в реестр телекоммуникационного оборудования российского происхождения (ТОРП), запись в реестр российских программ для ЭВМ и баз данных
xFirewall 5	Сертификация ФСТЭК России, отсутствие сертификата ФСБ, запись в реестр российских программ для ЭВМ и баз данных
Dionis DPS	Сертификация ФСТЭК России, отсутствие сертификата ФСБ, запись в реестр российских программ для ЭВМ и баз данных

Diamond VPN/FW	Сертификация ФСТЭК России, отсутствие сертификата ФСБ, запись в реестр российских программ для ЭВМ и баз данных

Рассматриваемые системы соответствуют требованиям по информационной безопасности, установленным ФСТЭК России, что подтверждается наличием соответствующих сертификатов у большинства решений, включая Ideco UTM, Континент 4, xFirewall 5, Dionis DPS и Diamond VPN/FW. Однако отсутствие сертификации ФСБ ограничивает их применение в ряде государственных или критически значимых объектов, где такие требования обязательны. Вместе с тем, включение UserGate, Континента 4 и xFirewall 5 в реестры отечественного телекоммуникационного оборудования и программных продуктов подчеркивает их соответствие политике импортозамещения и делает их более привлекательными для организаций, ориентированных на использование сертифицированных российских решений.

По критерию «Управление и мониторинг»:

- Все системы обеспечивают управление и мониторинг, включая интерфейс управления, мониторинг состояния, управление политиками безопасности и системы логирования.
- В целом, уровень управления и мониторинга в этих системах схож, что обеспечивает администраторам возможность эффективно управлять и следить за состоянием системы.

По критерию «Поддержка и обновления»:

- Все системы предоставляют регулярные обновления и поддержку через тикет-систему.

- Поддержка дополняется документацией и наличием обществ пользователей, что обеспечивает пользователям доступ к ресурсам и информации для решения проблем.

Цены и лицензирование для каждой системы устанавливаются индивидуально и зависят от версии, конфигурации и требований заказчика.

Все рассмотренные системы сертифицированы ФСТЭК России и имеют соответствие стандартам безопасности. Некоторые также включены в реестры российской радиоэлектронной продукции и телекоммуникационного оборудования.

В таблице 14 представлено сравнение систем межсетевого экранирования по критерию «Интеграция с другими системами».

Все системы обладают простым интерфейсом и удобством использования, что делает их доступными для широкого круга пользователей.

Все системы поддерживают интеграцию с различными платформами виртуализации, что обеспечивает их гибкость и применимость в разнообразных средах.

Таблица 14

Сравнение систем межсетевого экранирования по критерию «Интеграция с другими системами»

Система	Интеграция с другими системами
UserGate	Имеется интеграция с различными платформами

	виртуализации (Vmware, Hyper-V, VirtualBox, KVM, XenServer, OpenStack, Citrix, Oracle VM Server).
Ideco UTM	Имеется интеграция с платформами виртуализации, такими как VMware и Hyper-V.
Континент 4	Имеется интеграция с платформой виртуализации VMware.
xFirewall 5	Имеется интеграция с различными платформами виртуализации (Vmware, Hyper-V, VirtualBox, KVM, XenServer, OpenStack, Citrix, Oracle VM Server).
Dionis DPS	Имеется интеграция с платформами виртуализации VMware и Hyper-V.
Diamond VPN/FW	Имеется интеграция с платформой виртуализации VMware.

Сделаем сводную таблицу сравнения систем межсетевого экранирования по различным критериям – таблица 15.

Таблица 15

Сводная таблица сравнения систем межсетевого экранирования по различным критериям

Критерии	UserGate	Ideco UTM	Континент 4	xFirewall 5	Dionis DPS	Diamond VPN/FW
Производительность	Высокая	Средняя	Высокая	Высокая	Высокая	Высокая
Функциональность	Обширная	Обширная	Обширная	Обширная	Обширная	Обширная
Масштабируемость	Да	Да	Да	Да	Да	Да
Совместимость	Широкая	Широкая	Широкая	Широкая	Широкая	Ограниченная
Безопасность	Высокая	Высокая	Высокая	Высокая	Высокая	Высокая
Управление и мониторинг	Эффективное	Эффективное	Эффективное	Эффективное	Эффективное	Эффективное
Поддержка и обновления	Доступна	Доступна	Доступна	Доступна	Доступна	Доступна
Цена и лицензирование	Гибкая	Гибкая	Гибкая	Гибкая	Гибкая	Гибкая
Сертификации и соответствие	Есть	Есть	Есть	Есть	Есть	Есть
Интеграция с другими системами	Широкая	Широкая	Широкая	Широкая	Широкая	Ограниченная
Простота использования	Простая	Простая	Простая	Простая	Простая	Простая

В результате обобщённого анализа можно заключить, что все рассматриваемые системы демонстрируют высокий уровень производительности, масштабируемости, функциональной насыщенности и соответствия требованиям безопасности. Такие решения, как UserGate, Ideco UTM, Континент 4, xFirewall 5 и Dionis DPS, характеризуются высокой совместимостью и возможностями интеграции с внешними системами, что делает их универсальными для применения в корпоративной ИТ-инфраструктуре. В то же время Diamond VPN/FW, несмотря на достойные показатели производительности, ограничен в плане взаимодействия с другими программно-аппаратными средствами.

Все платформы предоставляют развитые механизмы управления, мониторинга, обновлений и технической поддержки, что обеспечивает надёжность эксплуатации и соответствие современным требованиям. Гибкость ценовой политики также делает большинство решений доступными для широкого круга организаций.

Выбор конкретной системы в условиях энергетической компании должен основываться на особенностях её инфраструктуры, уровне требуемой защищённости и задачах масштабирования. С учётом представленных характеристик можно рекомендовать UserGate как универсальное решение с акцентом на производительность и совместимость, Ideco UTM — для организаций с уравновешенными требованиями к безопасности и функциям, Континент 4 и xFirewall 5 — для сетей с высокой нагрузкой и потребностью в интеграции, Dionis DPS — в качестве масштабируемого решения для критически важных объектов, а Diamond VPN/FW — в

ситуациях, где ключевыми критериями остаются производительность и защита, но расширенная интеграция не является приоритетной.

В ходе анализа российских сетевых решений, таких как UserGate и Ideco UTM, было выявлено несколько ключевых ограничений и особенностей, которые важно учитывать при их использовании в энергетической компании.

Первое - ограниченная гибкость изменений правил.Один из заметных недостатков UserGate - необходимость перезагрузки устройства для внесения изменений в правила. Это может вызвать простои в работе сети, что критично для энергетических компаний, где непрерывная работа сети является приоритетом.

Второе - системы безопасности против сетевых устройства. Российские решения пока больше направлены на обеспечение безопасности, чем на функции сетевых устройств. Это важно учитывать при планировании внедрения, так как некоторые сценарии требуют более широких функциональных возможностей.

И, третье – это личный опыт. В процессе тестирования Ideco UTM выявлен интересный момент - при нестандартных сценариях настройки удаленного доступа удалось достичь стабильной работы, используя неочевидные настройки. Этот курьезный случай может быть полезен для инженеров, исследующих гибкие варианты настройки.

Таким образом, можно сделать выводы о необходимости с учётом уникальных особенностей каждой системы выбирать решение, соответствующее специфике задач энергетической компании. Важно учитывать как ограничения, так и возможности каждой системы при принятии решения о

внедрении в конкретной среде.

Выбор системы UserGate представляется обоснованным с точки зрения производительности, функциональности и соответствия требованиям безопасности. Решение демонстрирует высокую скорость обработки трафика даже при активированных механизмах защиты, что делает его подходящим для сред с интенсивной нагрузкой. Широкий набор встроенных функций позволяет не только организовать защиту внешнего периметра и сегментацию сети, но и обеспечить соответствие требованиям к защите ИСПДн и построение безопасных корпоративных сетей с использованием алгоритмов ГОСТ.

Наличие сертификации ФСТЭК с четвёртым классом защиты свидетельствует о соответствии UserGate установленным государственным требованиям к информационной безопасности, а возможность установки криптоускорителей дополнительно повышает эффективность обработки зашифрованного трафика. Совместимость с большинством современных платформ виртуализации и возможность установки на универсальные серверы обеспечивают гибкость развёртывания и лёгкость интеграции в существующую ИТ-инфраструктуру.

Средства мониторинга и управления, доступные в системе, позволяют администраторам контролировать состояние информационной среды в реальном времени, обеспечивая оперативную реакцию на инциденты. Постоянная работа над развитием функционала, включая внедрение аппаратного ускорения, делает систему актуальной с точки зрения технологического прогресса. Гибкий подход к лицензированию даёт возможность

подобрать оптимальный комплект по функциональности и стоимости, что повышает экономическую эффективность внедрения UserGate в корпоративную сеть.

Таким образом, UserGate предоставляет комплексное и масштабируемое решение с высокой производительностью, широкими функциональными возможностями и высоким уровнем безопасности, что делает его привлекательным выбором для энергетической компании.

2.3.2. Анализ структуры выбранной системы. Установка и настройка

Программно-аппаратные комплексы UserGate представлены несколькими сериями, каждая из которых ориентирована на определённые условия эксплуатации и масштаб защищаемой инфраструктуры. Так, серия C предназначена для небольших объектов и филиалов, серия X — для промышленных и уличных условий, а серия D обеспечивает защиту сетей малых и средних предприятий, включая организации с сотнями пользователей. Более мощные серии E и F рассчитаны на крупные структуры, такие как банки, заводы, ведомства и министерства, предоставляя функциональность на уровне дата-центров и высокую производительность с поддержкой виртуализации.

Для энергетической компании выбор модели межсетевого экрана напрямую зависит от объёмов и специфики её инфраструктуры. В случае ограниченного количества пользователей и распределённой структуры объектов, оптимальным решением становится серия D. Она сочетает в себе достаточную производительность, широкую совместимость с виртуальными платформами, соответствие требованиям информационной безопасности и доступную

стоимость. Это делает серию D подходящей для организации централизованной защиты сетей, эффективной фильтрации трафика и построения защищённых каналов связи. При этом поддержка сертификаций и наличие технической поддержки от производителя обеспечивают соответствие требованиям отрасли и надёжную эксплуатацию в условиях критической инфраструктуры.

Давайте проведем сравнение моделей D200 и D500 серии D межсетевых экранов UserGate (таблица 16, рисунок 9).

Таблица 16

Сравнение моделей D200 и D500 серии D межсетевых экранов UserGate

Характеристика	D200	D500
Производительность	Intel Celeron, 2 ГБ ОЗУ	Intel Core i5, 4 ГБ ОЗУ
Пропускная способность	До 400 Мбит/с	До 1 Гбит/с
Порты Ethernet	4	6 (2 SFP)
Хранилище SSD	32 ГБ	120 ГБ
Рабочая температура	0°C - 40°C	-40°C - 70°C
Цена	Более бюджетный	Обычно более дорогой
Область применения	Малые предприятия	Средние предприятия



Рисунок 9 - UserGate D200, D500

Выбор между D200 и D500 зависит от конкретных потребностей и масштаба сети энергетической компании. Поскольку для ЦОДу нужна высокая производительность, больше портов и возможность работы в сложных условиях, D500 является более подходящим вариантом. В котельных

достаточно более базовой конфигурации, поэтому D200 является оптимальным выбором.

Рассмотрим структуру системы межсетевого экранирования UserGate серии D.

Система включает модуль фильтрации трафика, обеспечивающий блокировку/разблокировку доступа к веб-ресурсам, фильтрацию содержимого веб-страниц и управление доступом к приложениям и протоколам. Также присутствует прокси-сервер, выполняющий кэширование данных для оптимизации скорости доступа и аутентификацию пользователей.

UserGate серии D	**Модуль фильтрации трафика**
	Прокси-сервер
	Модуль VPN
	Система обнаружения вторжений (IDS)
	Управление политиками безопасности
	Модуль управления пропускной способностью
	Интерфейс управления
	Модуль аутентификации
	Модуль безопасности
	Модуль мониторинга
	Модуль управления пользователями
	Модуль отчетности

Рисунок 10 - Структура UserGate серии D

Модуль VPN предоставляет возможность создания виртуальных частных сетей для безопасного удаленного доступа. Система обнаружения вторжений (IDS) отслеживает сетевую активность, обнаруживает и предотвращает потенциальные угрозы.

Управление политиками безопасности включает

определение правил фильтрации трафика и настройку правил доступа. Модуль управления пропускной способностью оптимизирует использование пропускной способности сети.

Интерфейс управления предоставляет веб-интерфейс для администрирования системы, отображение статистики и журналов событий. Модуль аутентификации поддерживает различные методы аутентификации пользователей, а модуль безопасности обеспечивает защиту от вредоносных программ и вирусов, а также механизмы шифрования для обеспечения безопасности передачи данных.

Модуль мониторинга собирает и анализирует данные о сетевой активности и производительности. Модуль управления пользователями позволяет создавать и управлять учетными записями пользователей, а модуль отчетности формирует отчеты о сетевой активности и событиях безопасности.

В приложении А рассмотрен процесс установки и настройки системы.

Таким образом, в приложении А рассмотрен процесс установки межсетевого экрана UserGate на виртуальной машине и выполнения минимально необходимых настроек для обеспечения работы сети Trusted с доступом в Интернет. Также, рассмотрены создание правил в разделах "Межсетевой экран", "NAT и маршрутизация" и "Пропускная способность". Описаны основные принципы создания политик в UserGate и принцип работы условий при формировании правил. Эти настройки обеспечивают гибкость и контроль для администраторов UserGate в обеспечении безопасности и маршрутизации трафика в сети.

В приложении Б рассматриваются шаги по созданию

локальных пользователей на устройстве UserGate, интеграции с Microsoft Active Directory через LDAP-коннектор и настройке captive-портала для идентификации пользователей. Также рассмотрим раздел "Политики безопасности" в контексте функций "Инспектирование SSL", "Фильтрация контента" и "Веб-безопасность" в системе UserGate. В итоге, рассмотрим процесс предоставления удаленного доступа к внутренним ресурсам компании с использованием инструментов UserGate. Сфокусируемся на настройке Remote Access VPN и SSL VPN, предоставляя детальные шаги для обоих подходов.

В приложении Б были рассмотрены ключевые шаги по созданию и идентификации пользователей в UserGate. От создания локальных пользователей и групп до интеграции с Active Directory через LDAP-коннектор и настройки Captive-портала для дополнительной авторизации. Также, проанализировали разделы "Фильтрация контента", "Веб-безопасность" и "Инспектирование SSL" в UserGate. Эти аспекты представляют собой критически важные компоненты современных систем безопасности, являясь неотъемлемой частью современных средств защиты сетей. Их корректная настройка и использование существенно повышают уровень безопасности и эффективности сетевых ресурсов. Подробно рассмотрены процессы настройки удаленного доступа к внутренним ресурсам компании через Remote Access VPN в UserGate. Оба метода, Remote Access VPN и SSL VPN, предоставляют гибкие и безопасные варианты удаленного доступа, соответствуя потребностям современной корпоративной сетевой безопасности. В результате, были рассмотрены детали настройки профилей

безопасности VPN, создания сетей VPN, серверных правил, и настройки клиентов как на Windows, так и на Linux системах. Также был представлен вариант использования веб-портала для предоставления доступа к внутренним ресурсам через протокол HTTPS. Оба метода, Remote Access VPN и SSL VPN, предоставляют эффективные средства удаленного доступа к внутренней инфраструктуре компании, обеспечивая безопасность и гибкость настроек.

С учетом необходимых мер, схема аппаратного обеспечения системы информационной защиты организации приведена на рис. 11. На рис. 12 приведена схема программного обеспечения системы информационной защиты диспетчерской предприятия.

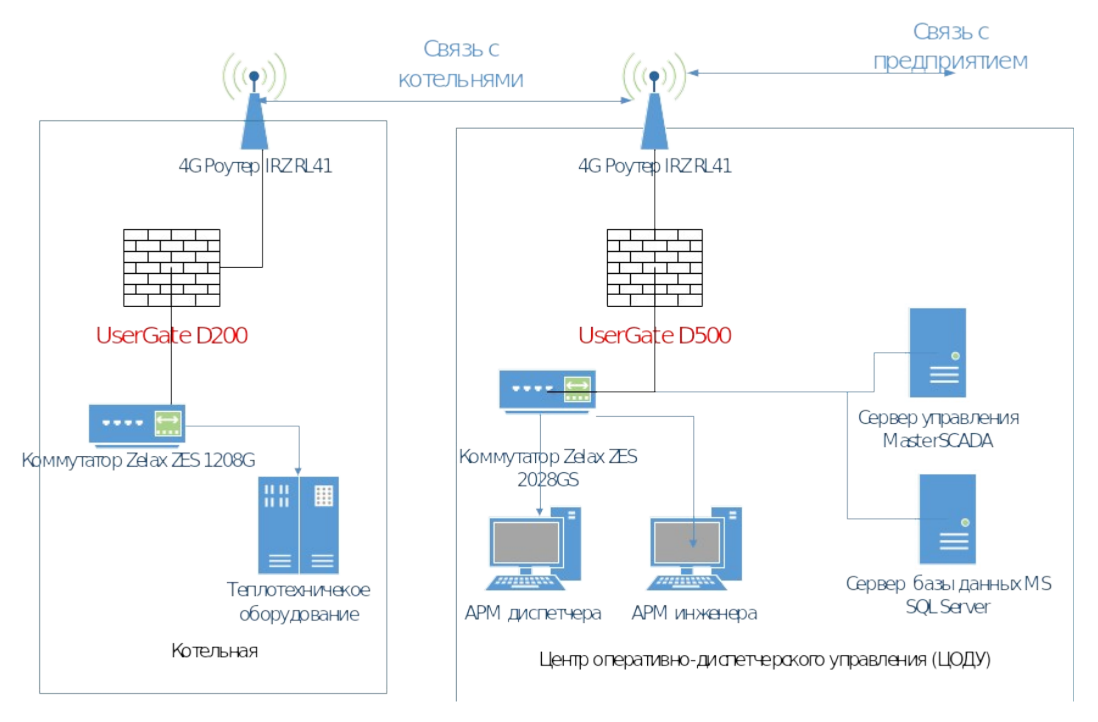


Рисунок 11 - Схема аппаратного обеспечения информационной системы

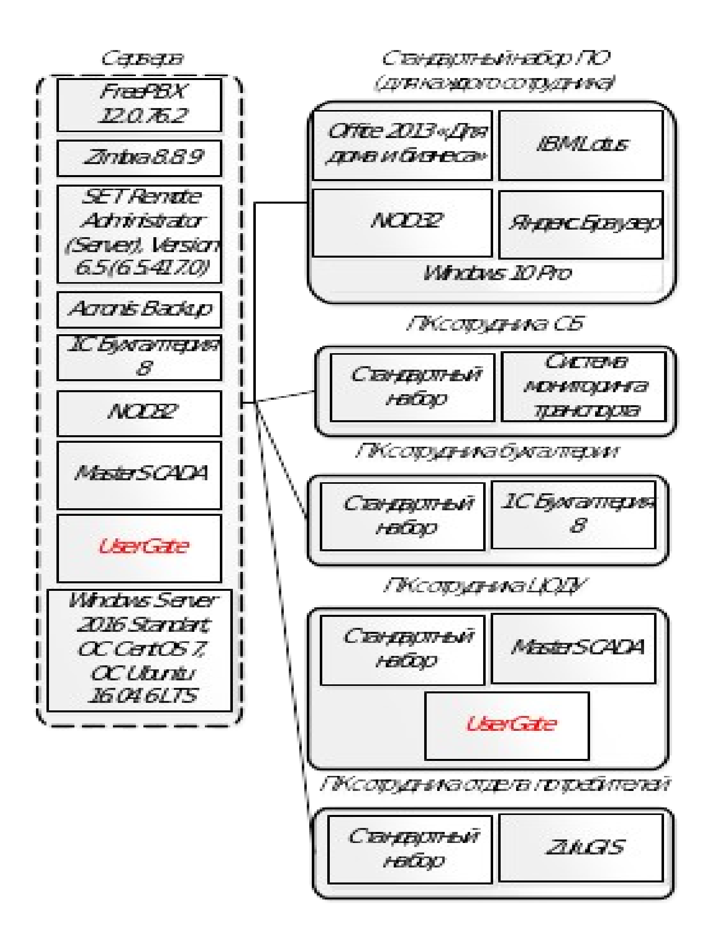


Рисунок 12 - Схема программного обеспечения информационной системы предприятия

2.3.3. Обоснование экономической эффективности внедрения системы межсетевого экранирования в компании

Отправной предпосылкой при экономической эффективности считают практически неоспоримое мнение: с одной стороны, при нарушении защищенности информации наносится некоторый ущерб, а с другой - для обеспечения надежной защиты информации требуются затраты финансовых средств. Совокупная предполагаемая стоимость защиты выражается как сумма затраченных средств на защиту и ущерба от ее нарушения.

Оптимальным решением можно считать направление на

защиту информации денежных средств, которые уменьшают суммарную стоимость работ, связанных с защитой информации.

Экономическую рентабельность мер, обеспечивающих защиту информации, можно определить через размер предотвращенного убытка или величину снижения риска для информационных активов организации.

Для применения данного подхода при решении проблемы, необходимо знать:

– первое: предполагаемые потери при нарушении защищенности информации;

– второе: зависимость между степенью защищенности и средствами, затрачиваемыми на меры, связанные с защитой информации.

Для определения уровня затрат R_i, который способен обеспечить необходимую степень защищенности информации, необходимо знать:

- – первое: перечень всех без исключения угроз информации;
- – второе: вероятную опасность для информации для любой угрозы;
- – третье: объемы расходов, необходимые для нейтрализации каждой угрозы.

Поскольку оптимальное решение вопроса о рациональном объеме затрат на защиту состоит в том, что данный объем должен быть равен величине предполагаемых потерь при нарушении защищенности, будет достаточным определение только степени потерь. В качестве одной из методик определения уровню затрат может применяться

такая эмпирическая зависимость предполагаемых потерь (рисков) от i-й угрозы информации:

$$R_i = 10^{(Si + Vi - 4)} \quad (1)$$

где: Si является коэффициентом, характеризующим возможную частоту появления соответствующей угрозы; а

Vi - коэффициентом, характеризующим значение возможного ущерба при ее возникновении.

Для расчета выбраны 4 наиболее ценных актива электроэнергетической компании. Также были взяты и соответствующие им угрозы, которым присвоена оценка «высокая».

Рассмотрим пример расчета размера потерь для информационного актива о предоставляемых услугах и угрозы для него - перехватывание информации:

1) при помощи шкалы предполагаемой частоты появления угрозы, выбираем рассчитываемое значение $Si=5$ (1 раз в месяц, за год примерно 10 раз);

2) при помощи шкалы предполагаемого значения возможного ущерба при появлении угрозы, выбираем рассчитываемое значение $Vi=4$ (300 тыс. руб.).

3) в формулу подставим значение:

$R_i = 10^{(5+4-4)}$;

R_i = 100,000 руб.

Вследствие расчета можно определить общую стоимость потерь, используя формулу:

$$R = \sum_{i=1}^{N} R_i \quad (2)$$

где N является количеством угроз информационным активам, которые определены ранее; следует заметить, что

общая стоимость потерь рассчитывается для каждого актива отдельно.

Рассмотрим пример расчета общей величины потери для информационного актива о финансовых отчетах организации:

1) N = 4; так как собственно 4-м угрозам для этого актива присвоена оценка «высокая»;

2) R_i = 310,000 (100,000 + 100,000 + 100,000+ 10,000);

3) в формулу подставим значения:

$R=\sum_{i=1}^{4} 310,000$, $R=$ 1,240,000 руб.

Расчет для всех наиболее ценных активов и соответствующих для них угроз представлен в таблице 17.

Таблица 17

Величины потерь для критичных информационных ресурсов до модернизации системы защиты информации

Актив	Угроза	Величина потерь (руб.)
Финансовые отчеты компании	Зависимость от партнеров/клиентов	100,000
	Нарушения договорных обязательств посторонними (третьими) лицами	100,000
	Ошибки в обеспечении безопасности информационных систем на этапах жизненного цикла	100,000
	Применение программных средств и информации без гарантии источника	10,000
Персональные данные сотрудников	Ошибки, которые допущены при заключении контрактов с провайдерами внешних услуг	10,000
	Разработка и применение некачественной документации	10,000
	Несанкционированный логический доступ	10,000
Система обеспечения безопасности компании	Нарушения договорных обязательств посторонними (третьими) лицами	10,000
	Разрушение/повреждение, аварии технических средств и каналов связи	10,000
Сведения о схемах размещения систем безопасности	Халатность	10,000
	Выполнение вредоносных программ	10,000
	Действия неавторизованного субъекта	10,000
Суммарная величина потерь		1,460,000

Денежную меру считают предельно общим типом представления ресурса. Ресурс, выделен для защиты информации, может иметь разовый и постоянный характер. Объем и содержание разового ресурса, выделенного для защиты информации в электроэнергетической компании представлен в таблице 18.

Объем и содержание постоянного ресурса, который выделен для защиты информации в электроэнергетической компании представлен в таблице 19.

Общее значение ресурса, выделенного для защиты информации в электроэнергетической компании, составляет 903,124 тыс. рублей (369,924+523,20).

Таблица 18

Объем и содержание разового ресурса, выделенного для защиты

Организационные мероприятия				
№ п\п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час)	Стоимость, всего (руб.)
1	Установка и настройка UserGate	5000,00	1\2	10000,00
Стоимость проведения организационных мероприятий, всего				10000,00
Мероприятия инженерно-технической защиты				
№ п\п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (руб)	Кол-во (ед.измерения)	Стоимость, всего (руб.)
1	UserGate D200	19746,00	15 шт.	296190,00
2	UserGat D500	31867,00	2 шт.	63734,00
Стоимость проведения мероприятий инженерно-технической защиты				359924,00
Объем разового ресурса, выделяемого на защиту информации (тыс.руб.)				369,924

Таблица 19

Объем и содержание постоянного ресурса, выделенного для защиты

Организационные мероприятия				
№	Выполняемые действия	Среднечасова	Трудоемкость	Стоимость,

п\п		я зарплата специалиста (руб.)	операции (чел.час)	всего (тыс. руб.)
1	Заработная плата администратора ИБ	220,00	1\2160	475,20
2	Обучение и повышение профессиональных навыков	40,00	6\100	24,00
3	Организационные мероприятия по обучению пользователей	40,00	6\100	24,00
Стоимость проведения организационных мероприятий, всего				523,20
Мероприятия инженерно-технической защиты				
№ п\п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (руб)	Кол-во (ед.измерения)	Стоимость, всего (руб.)
1	-	-	-	-
Стоимость проведения мероприятий инженерно-технической защиты				-
Объем разового ресурса, выделяемого на защиту информации				523,20

Таблица 20

Величины потерь для критических информационных ресурсов по окончанию модернизации системы по защите информации с помощью системы межсетевого экранирования

Актив	Угроза	Величина потерь (руб.)
Финансовые отчеты компании	Зависимость от партнеров/клиентов	10,000
	Нарушения договорных обязательств сторонними (третьими) лицами	1,000
	Ошибки в обеспечении безопасности информационных систем на этапах жизненного цикла	1,000
	Применение программных средств и информации без гарантии источника	1,000
Персональные данные сотрудников	Ошибки, которые допущены при заключении контрактов с провайдерами внешних услуг	1,000
	Разработка и применение некачественной документации	1,000
	Несанкционированный логический доступ	1,000
Система обеспечения безопасности компании	Нарушения договорных обязательств сторонними (третьими) лицами	1,000
	Разрушение/повреждение, аварии технических средств и	100

	каналов связи	
Сведения о схемах размещения систем безопасности	Халатность	1,000
	Выполнение вредоносных программ	100
	Действия неавторизованного субъекта	100
Суммарная величина потерь		66,800

Рассмотрим расчет длительности окупаемости модернизируемой системы по защите информации с помощью системы межсетевого экранирования, который проводился аналитическим и графическим методом. Для этого необходимо получить предполагаемые данные о величине потерь для критических информационных ресурсов по окончанию модернизации системы по защите информации с помощью системы межсетевого экранирования, см. таблицу 20.

Оценка динамичности величин потерь за срок не менее 1 года приведена в таблице 21.

Проведем расчет длительности окупаемости системы ($T_{ок}$), используя формулу:

$$T_{ок}=R\sum ¿(R_{ср}-R_{прогн})$$

$$T_{ок}=903,124/(1,460,000-66,800)$$

$$T_{ок}=0,64$$

Таблица 21

Оценка динамики величин потерь (тыс. руб.)

	1 кв.	2 кв.	3 кв.	1 год	1 кв.	2 кв.	3 кв.	2 год
До внедрения СЗИ	5,703125	11,40625	22,813	45,625	91,25	182,5	365	730
После внедрения СЗИ	0,2609375	0,521875	1,0438	2,0875	4,175	8,35	16,7	33,4
Снижение потерь	5,4421875	10,88438	21,769	43,538	87,075	174,15	348,3	696,6

Полученный графическим способом расчет изображен на рисунке 13.

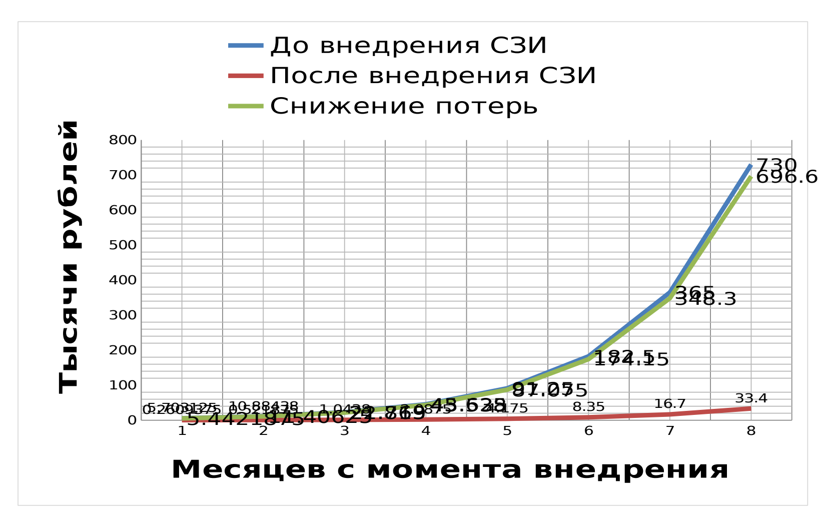


Рисунок 13 - Динамика потерь

По результатам проведенных расчетов можно прийти к выводу, что внедряемое средство по защите информации с помощью системы межсетевого экранирования начинает себя окупать практически сразу, а полностью окупит себя примерно через семь месяцев, что позволит существенно уменьшить финансовые потери электроэнергетической компании в случае появления угроз информационной безопасности с помощью системы межсетевого экранирования.

Выводы по главе

В результате выполнения главы проведен анализ и выбор модели программно-аппаратного комплекса UserGate, описана структура данной выбранной системы межсетевого экранирования, проведена установка, настройка и анализ

работы системы, а также обоснована экономическая эффективность проекта.

Поскольку для ЦОДу нужна высокая производительность, больше портов и возможность работы в сложных условиях, D500 является более подходящим вариантом. В котельных достаточно более базовой конфигурации, поэтому D200 является оптимальным выбором.

Рассмотрен процесс установки межсетевого экрана UserGate на виртуальной машине и выполнения минимально необходимых настроек для обеспечения работы сети Trusted с доступом в Интернет. Проведено создание правил в разделах "Межсетевой экран", "NAT и маршрутизация" и "Пропускная способность". Описаны основные принципы создания политик в UserGate и принцип работы условий при формировании правил. Эти настройки обеспечивают гибкость и контроль для администраторов UserGate в обеспечении безопасности и маршрутизации трафика в сети. Были рассмотрены ключевые шаги по созданию и идентификации пользователей в UserGate.

ЗАКЛЮЧЕНИЕ

В результате выполнения работы проведено исследование направлений совершенствования информационной безопасности автоматизированных систем и сетей в АО «Системный оператор Единой энергетической системы» путем импортозамещения и внедрение системы межсетевого экранирования в электроэнергетической компании. Для этого проведена техническая и экономическая характеристика предметной области рассматриваемого предприятия, проанализированы риски информационной безопасности предприятия, дана характеристика комплексу задач, задаче и обоснованию необходимости в усовершенствовании системы межсетевого экранирования на рассматриваемом предприятии. В результате чего проведен анализ, выбор и описание внедрения отечественных систем межсетевого экранирования и обоснована экономическая эффективность разработанного проекта.

В первой главе работы предоставлена аргументация актуальности выбора задачи по обеспечению информационной безопасности, аргументирована и изложена применяемая стратегия действий, связанных с защитой информационных ресурсов, итоги анализа предметной области, аргументация и итоги выбора инженерно-технических и административных мер.

Использование отечественных систем межсетевого экранирования в электроэнергетической компании обосновано повышенной адаптацией к местным условиям и

угрозам, соблюдением законодательства, эффективной локальной поддержкой, развитием отечественной индустрии информационной безопасности и обеспечивает геополитическую независимость компании.

Исследование в области использования отечественных систем межсетевого экранирования в электроэнергетической компании имеет как научную новизну, так и практическую значимость.

Исследование в области применения отечественных систем межсетевого экранирования в электроэнергетической компании обрело научную новизну через адаптацию технологий к местным условиям и угрозам, выявление и устранение потенциальных уязвимостей, а также оценку эффективности средств защиты.

Научная новизна:

- Адаптация к местным условиям - глубокий анализ и адаптация систем под конкретные местные угрозы и требования, что может привести к созданию инновационных решений в области кибербезопасности.
- Исследование уязвимостей - идентификация потенциальных уязвимостей в отечественных системах и предложение инновационных методов их устранения или смягчения.
- Эффективность средств защиты - оценка эффективности российских систем межсетевого экранирования с точки зрения предотвращения различных видов кибератак, что может стать объектом научного интереса.

Практическая значимость исследования заключается в улучшении кибербезопасности энергетической компании,

обеспечении соответствия нормативам в области информационной безопасности, реализации экономических выгод от использования отечественных систем и поддержке развития национальной индустрии информационной безопасности.

Практическая значимость:

- Улучшение кибербезопасности - разработка и внедрение эффективных средств защиты, способных эффективно сопротивляться современным киберугрозам.
- Соблюдение нормативов - предоставление решений, соответствующих местным и международным нормативам в области кибербезопасности для энергетических компаний.
- Экономический эффект - оценка экономических выгод от использования отечественных систем в сравнении с импортными, что может стать основой для принятия решений о внедрении таких систем в других компаниях.
- Развитие отечественной отрасли - поддержка российских производителей способствует развитию национальной индустрии информационной безопасности, что имеет важное значение для экономики страны.

Таким образом, исследование внесет вклад как в расширение научных знаний в области кибербезопасности, так и в улучшение практических аспектов обеспечения безопасности в энергетических компаниях.

Во второй главе проведен анализ возможностей, преимущества, недостатки и сравнение таких отечественных систем: Usergate; Ideco UTM; Континент 4; xFirewall 5; Dionis DPS; Diamond VPN/FW.

Выделены такие критерия для сравнения как: безопасность, управление и мониторинг, функциональность,

производительность, поддержка и обновления, цена и лицензирование, сертификации и соответствие, интеграция с другими системами, простота использования, масштабируемость, совместимость.

Исследование позволило рассмотреть несколько решений для обеспечения безопасности и управления сетями в энергетической компании:

- UserGate выделяется высокой производительностью, обширным функционалом, сертификацией от ФСТЭК России и поддержкой алгоритмов ГОСТ для шифрования. Система гибкая и совместима с различными платформами виртуализации.
- Ideco UTM привлекает своей универсальностью и широким спектром функций безопасности, но нужно учесть отсутствие поддержки алгоритмов ГОСТ.
- Континент 4 обеспечивает высокую производительность и сертификацию от ФСТЭК России, но некоторые ограничения в поддержке виртуализации.
- xFirewall 5 предоставляет широкий функционал, но ограничен в поддержке алгоритмов ГОСТ и совместимости с платформами виртуализации.
- Dionis DPS выделяется своей масштабируемостью и высокой производительностью, но не имеет сертификации от ФСТЭК России.
- Diamond VPN/FW имеет широкий спектр возможностей, но нужно учитывать ограничения в поддержке алгоритмов ГОСТ.

В результате проведенного сравнительного анализа выбрана система межсетевого экранирования UserGate – это комплексное решение, которое выделяется высокой

производительностью, обширным функционалом и высоким уровнем безопасности. Сертификация от ФСТЭК России с классом защиты 4 подтверждает надежность системы. Поддержка создания защищенной корпоративной сети и шифрования трафика в VPN с использованием алгоритмов ГОСТ обеспечивает безопасность передачи данных. UserGate совместим с различными платформами виртуализации, обеспечивая гибкость в установке. Удобное управление и мониторинг, а также регулярные обновления делают его привлекательным решением для энергетических компаний.

В результате выполнения третьей главы проведен анализ и выбор модели программно-аппаратного комплекса UserGate, описана структура данной выбранной системы межсетевого экранирования, проведена установка, настройка и анализ работы системы, а также обоснована экономическая эффективность проекта.

Поскольку для ЦОДу нужна высокая производительность, больше портов и возможность работы в сложных условиях, D500 является более подходящим вариантом. В котельных достаточно более базовой конфигурации, поэтому D200 является оптимальным выбором.

Рассмотрен процесс установки межсетевого экрана UserGate на виртуальной машине и выполнения минимально необходимых настроек для обеспечения работы сети Trusted с доступом в Интернет. Проведено создание правил в разделах "Межсетевой экран", "NAT и маршрутизация" и "Пропускная способность". Описаны основные принципы создания политик в UserGate и принцип работы условий при формировании правил. Эти настройки обеспечивают гибкость

и контроль для администраторов UserGate в обеспечении безопасности и маршрутизации трафика в сети.

Были рассмотрены ключевые шаги по созданию и идентификации пользователей в UserGate. От создания локальных пользователей и групп до интеграции с Active Directory через LDAP-коннектор и настройки Captive-портала для дополнительной авторизации. Также, проанализировали разделы "Фильтрация контента", "Веб-безопасность" и "Инспектирование SSL" в UserGate. Эти аспекты представляют собой критически важные компоненты современных систем безопасности, являясь неотъемлемой частью современных средств защиты сетей. Их корректная настройка и использование существенно повышают уровень безопасности и эффективности сетевых ресурсов. Подробно рассмотрены процессы настройки удаленного доступа к внутренним ресурсам компании через Remote Access VPN в UserGate. Оба метода, Remote Access VPN и SSL VPN, предоставляют гибкие и безопасные варианты удаленного доступа, соответствуя потребностям современной корпоративной сетевой безопасности. В результате, были рассмотрены детали настройки профилей безопасности VPN, создания сетей VPN, серверных правил, и настройки клиентов как на Windows, так и на Linux системах. Также был представлен вариант использования веб-портала для предоставления доступа к внутренним ресурсам через протокол HTTPS. Оба метода, Remote Access VPN и SSL VPN, предоставляют эффективные средства удаленного доступа к внутренней инфраструктуре компании, обеспечивая безопасность и гибкость настроек.

По результатам проведенных расчетов экономической

эффективности можно прийти к выводу, что внедряемое средство по защите информации с помощью системы межсетевого экранирования начинает себя окупать практически сразу, а полностью окупит себя примерно через семь месяцев, что позволит существенно уменьшить финансовые потери электроэнергетической компании в случае появления угроз информационной безопасности с помощью системы межсетевого экранирования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Президент РФ: Указ от 30.03.2022 №166 О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ"
2. Бегаев А.Н., Кашин С.В., Маркевич Н.А., Марченко А.А. Выявление уязвимостей и недекларированных возможностей в программном обеспечении. Учебно-методическое пособие. – СПб: Университет ИТМО, 2020. – 38 с.
3. Богульская Н.А., Кучеров М.М. Модели безопасности компьютерных систем. - Красноярск: СГУ, 2019. — 207 с.
4. Бузов Г.А. Выявление специальных технических средств несанкционированного получения информации. - М.: Горячая линия – Телеком, 2019. — 204 с.: ил. — ISBN 978-5-9912-0795-9
5. Васильева И.Н., Федоров Д.Ю. Интеллектуальные системы защиты информации. - СПб.: СПбГЭУ, 2020. — 120 с.
6. Вострецова Е.В. Основы информационной безопасности. Учебное пособие. — Екатеринбург: Уральский

федеральный университет им. Первого президента России Б.Н. Ельцина (УрФУ), 2019. — 204 с. — ISBN 978-5-7996-2677-8

7. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации. 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.

8. Гузенкова Е.А., Паршин К.А. Программно-аппаратная защита информации. Конспект лекций. — Екатеринбург: Уральский государственный университет путей сообщения, 2019. — 87 с.

9. Душкин А.В. (ред.) Программно-аппаратные средства обеспечения информационной безопасности. Практикум. Учебное пособие.— Москва: Горячая линия - Телеком, 2019. — 412 с. — ISBN 978-5-9912-0797-3

10. Еськин Д.Л., Бакулин В.М. Основы защиты информации в компьютерных системах и сетях. - Волгоград : ВА МВД России, 2019. – 68с.

11. Зимин И.В. Информационная безопасность. Учебное пособие. — Бишкек: Кыргызско-Российский Славянский университет (КРСУ), 2018. — 132 с. — ISBN 978-9967-19-555-4

12. Зырянова Т.Ю. Информационная безопасность и защита информации. Конспект лекций. — Екатеринбург: Уральский государственный университет путей сообщения, 2019. — 142 с.

13. Иванцов А.М., Козловский В.Г. Основы информационной безопасности. Курс лекций в 2 частях. Часть 1. Учебное пособие. — Ульяновск: Ульяновский государственный университет, 2019. — 72 с.

14. Ищейнов В.Я. Информационная безопасность и защита информации. - Москва ; Берлин : Директ-Медиа, 2020. — 270 с. — ISBN 978-5-4499-0496-6

15. Ищейнов В.Я. Информационная безопасность и защита информации. Словарь терминов и понятий. - М.: Русайнс, 2021. — 226 с. — ISBN 798-5-4365-5672-7

16. Климентьев К.Е. Введение в защиту компьютерной информации. Учебное пособие. — Самара: Самарский национальный исследовательский университет им. академика С.П. Королева, 2020. — 183 с. — ISBN 978-5-7883-1526-3

17. Костин В.Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей. - Москва: Изд. Дом НИТУ МИСиС, 2018. — 31 с. — ISBN 978-5-906053-53-7

18. Лившиц И.И. Экономическое обеспечение информационной безопасности. - Учебно-методическое пособие. — СПб: Университет ИТМО, 2021. – 69 с.

19. Лойко В.И., Лаптев В.Н., Аршинов Г.А., Лаптев С.В. Информационная безопасность. - Учебное пособие. – Краснодар: КубГАУ, 2020. – 332 с. ISBN 978-5-907346-50-5

20. Насонова Н.В., Пухир Г.А., Петров С.Н. Основы защиты информации. Учебно-методическое пособие. — Минск: Белорусский государственный университет информатики и радиоэлектроники, 2019. — 83 с. — ISBN 978-985-543-437-6

21. Парфёнов Ю.П. Средства управления и защиты информационных ресурсов автоматизированных систем. Учебное пособие. — Екатеринбург: Уральский федеральный университет им. первого Президента России Б.Н. Ельцина (УрФУ), 2020. — 120 с. — ISBN 978-5-7996-3088-1

22. Полегенько А.М. Защита информационных систем обработки персональных данных. Учебное пособие. — СПб.: Санкт-Петербургский государственный экономический университет, 2018. — 72 с. — ISBN 978-5-7310-4510-0

23. Сафонова В.Ю. Основы информационной безопасности. 2-е изд. — Оренбург: ОГПУ, 2018. — 176 с. — ISBN 9785907075054

24. Сидоренко В.Г., Скоробогатова Н.Н. Аспекты информационной безопасности. Учебное пособие. — М.: Российский университет транспорта (МИИТ). 2018. — 64 с.

25. Скабцов Никита. Аудит безопасности информационных систем. - СПб.: Питер, 2018. — 272 с. — (Библиотека программиста). — ISBN 978-5-4461-0662-2

26. Солонская О.И. Средства защиты информации. - Новосибирск : СибГУТИ, 2021. — 89 с.

27. Сухостат В.В., Васильева И.Н. Основы информационной безопасности. Учебное пособие. — СПб.: СПбГЭУ, 2019. — 103 с. — ISBN 978-5-7310-4634-3

28. Тесленко И.Б., Виноградов Д.В., Губернаторов А.М. и др. Информационная безопасность. Учебное пособие. — Владимир: Владимирский государственный университет им. А.Г. и Н.Г. Столетовых (ВлГУ), 2023. — 212 с. — ISBN 978-5-9984-1783-2.

29. Форшоу Д. Атака сетей на уровне протоколов. Руководство хакера по перехвату и анализу сетевого трафика и эксплуатации уязвимостей. - М.: ДМК Пресс, 2021. — 340 с. — ISBN 978-5-97060-972-9.

30. Хаббард Дуглас У., Сирсен Ричард. Как оценить риски в кибербезопасности. Лучшие инструменты и практики. - М.: Эксмо, 2023. — 439 с.

31. Хоффман Эндрю. Безопасность веб-приложений. Разведка, защита, нападение. - СПб.: Питер, 2021. — 336 с.: ил. — (Бестселлеры O'Reilly). — ISBN 978-5-4461-1786-4.

32. Чио Кларенс, Фримэн Дэвид. Машинное обучение и безопасность. Пер. с англ. А.В. Снастина. — Москва: ДМК Пресс, 2020. — 388 с. — ISBN: 978-5-97060-713-8.

33. Шварцкоп О.Н., Хабибуллин Ф.Х. Информационная безопасность в профессиональном образовании. Учебно-методическое пособие. — Челябинск: Издательство ЗАО «Библиотека А.Миллера», 2020 – 75 с.

34. Энсон С. Реагирование на компьютерные инциденты. Прикладной курс. — Пер. с англ. Д. А. Беликова. — М.: ДМК Пресс, 2021. — 436 с.: ил. — ISBN 978-5-97060-484-7.

35. UserGate документация [Электронный ресурс] // UserGate. – URL: https://docs.usergate.com/dokumentaciya-120/ (дата обращения: 29.06.2025 г.).

Приложение А. Установка и настройка системы

Система UserGate предоставляется в виде программно-аппаратного комплекса, который может быть развернут в виртуальной среде. Для начала установки, необходимо скачать образ в формате OVF (Open Virtualization Format) из личного кабинета на сайте UserGate. Этот формат совместим с виртуализационными платформами VMWare и Oracle Virtualbox. Для Microsoft Hyper-V и KVM предоставляются образы дисков виртуальной машины.

Для корректной работы виртуальной машины рекомендуется использовать минимум 8GB оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать 64-битные операционные системы. Установка начинается с импорта образа в выбранный гипервизор (VirtualBox и VMWare). В случае Microsoft Hyper-V и KVM, необходимо создать виртуальную машину и указать в качестве диска скачанный образ, а затем отключить службы интеграции в настройках созданной виртуальной машины.

После импорта в VMWare создается виртуальная машина с рекомендованными настройками (рисунок А.1). Оперативной памяти должно быть не менее 8GB, с увеличением на 1GB на каждые 100 пользователей. Размер жесткого диска по умолчанию – 100GB, но для хранения всех журналов и настроек рекомендуется использовать 300GB или более.

UserGate UTM поставляется с четырьмя интерфейсами, назначенными в зоны: Management, Trusted, Untrusted, и DMZ. Затем запускается виртуальная машина, где UTM

настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске (рисунок А.2).

Для доступа к веб-интерфейсу UserGate используется Management-интерфейс (eth0), который настроен на получение IP-адреса в автоматическом режиме. Если необходимо назначить адрес вручную, это можно сделать через CLI (Command Line Interface) (рисунок А.3).

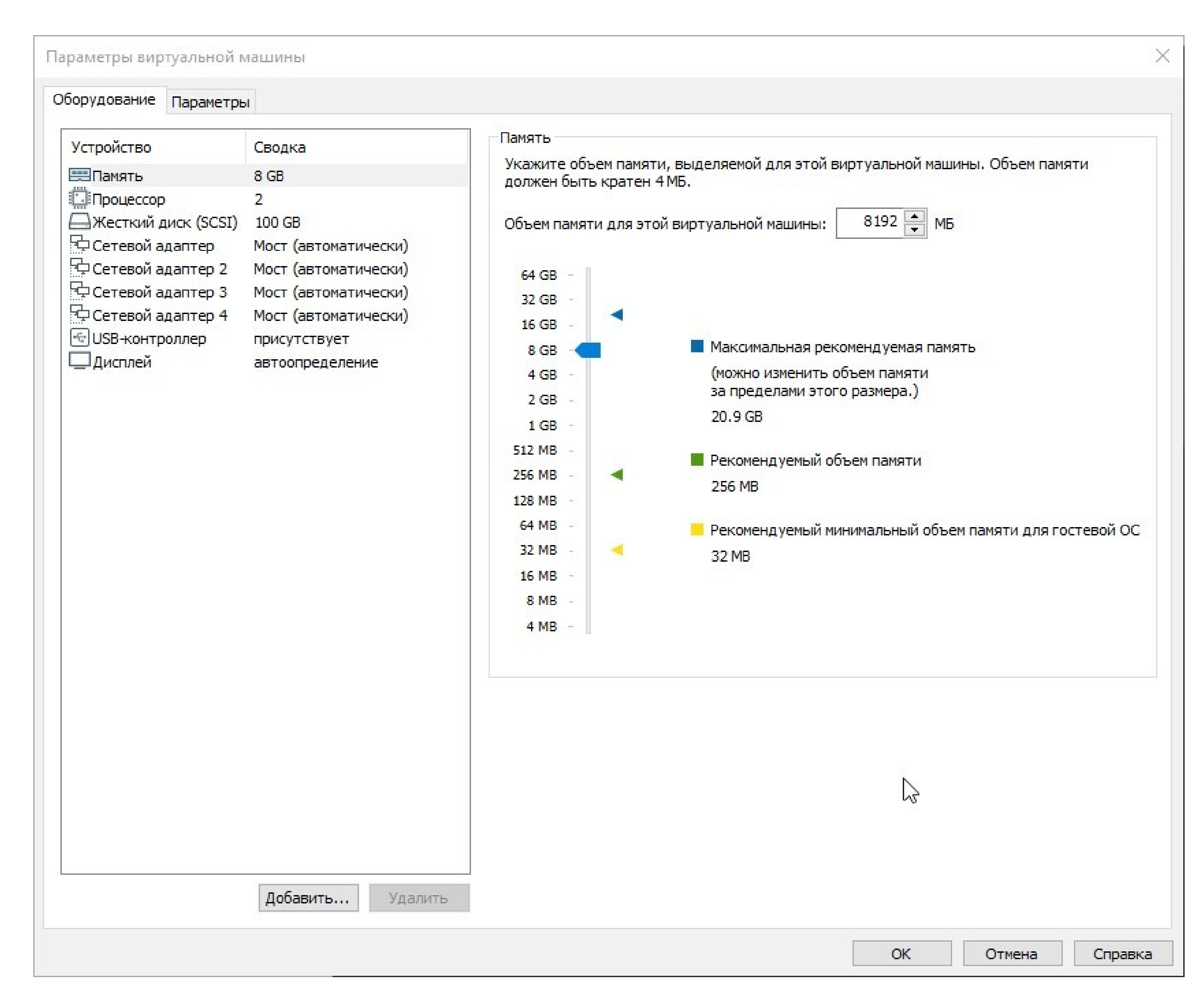


Рисунок А.1. Рекомендуемые настройки виртуальной машины



Рисунок А.2. Выбор UTM

```
UserGate UTM 5.0.6.4337R-1

Web-administrator GUI: https://192.168.1.136:8001/
Non-transparent HTTP(S) proxy: 192.168.1.136:8090

ugutm login: _
```

Рисунок А.3. Работа через CLI

Установка продолжается через веб-консоль, где выбираются язык интерфейса, часовой пояс, и соглашение с лицензией. Далее устанавливаются логин и пароль для входа в веб-интерфейс управления (рисунок А.4).

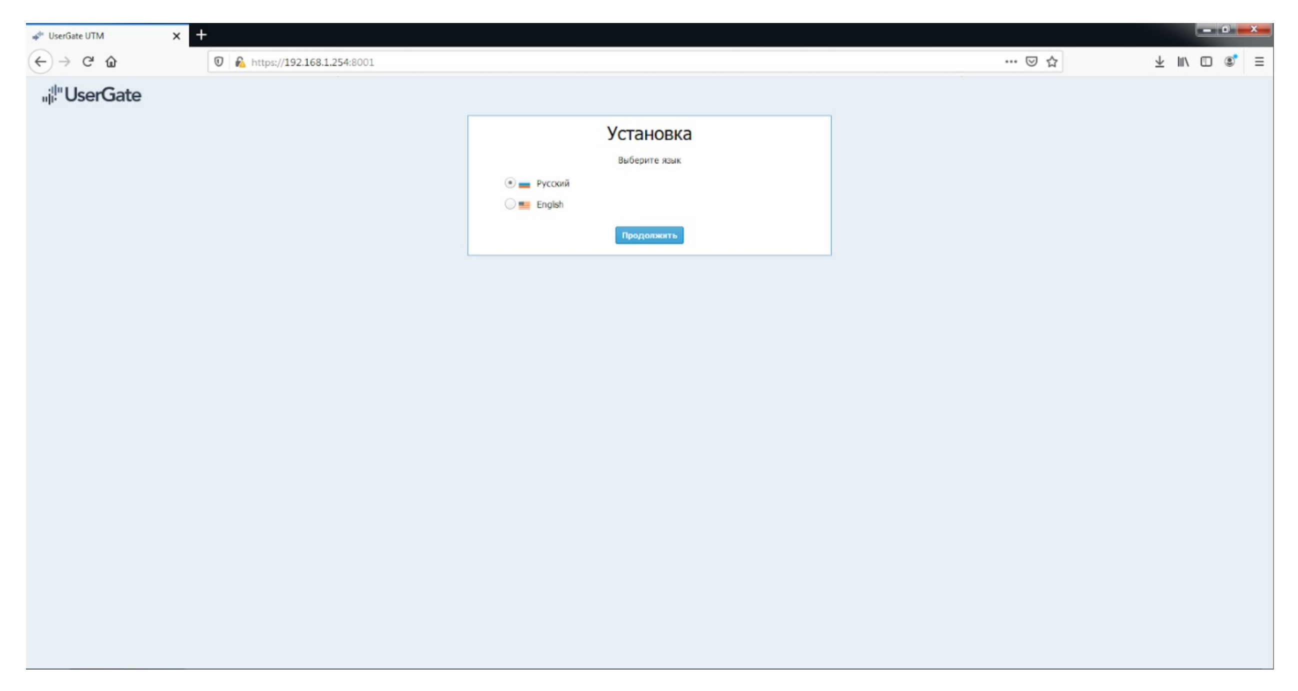


Рисунок А.4. Веб-консоль UserGate

Настройка системы включает в себя управление интерфейсами, настройку шлюзов, добавление DNS серверов и другие параметры (рисунок А.5). Раздел "Интерфейсы" позволяет включить и настроить физические и виртуальные интерфейсы (рисунок А.6). Администраторы UserGate имеют возможность редактировать параметры зон, которые предоставляются по умолчанию, и также создавать дополнительные зоны (рисунок А.7). Затем настраивается маршрут по умолчанию через раздел "Шлюзы" (рисунок А.8). Раздел "DNS" предоставляет возможность добавить DNS сервера и настроить DNS-прокси для изменения DNS-запросов от пользователей (рисунок А.9).

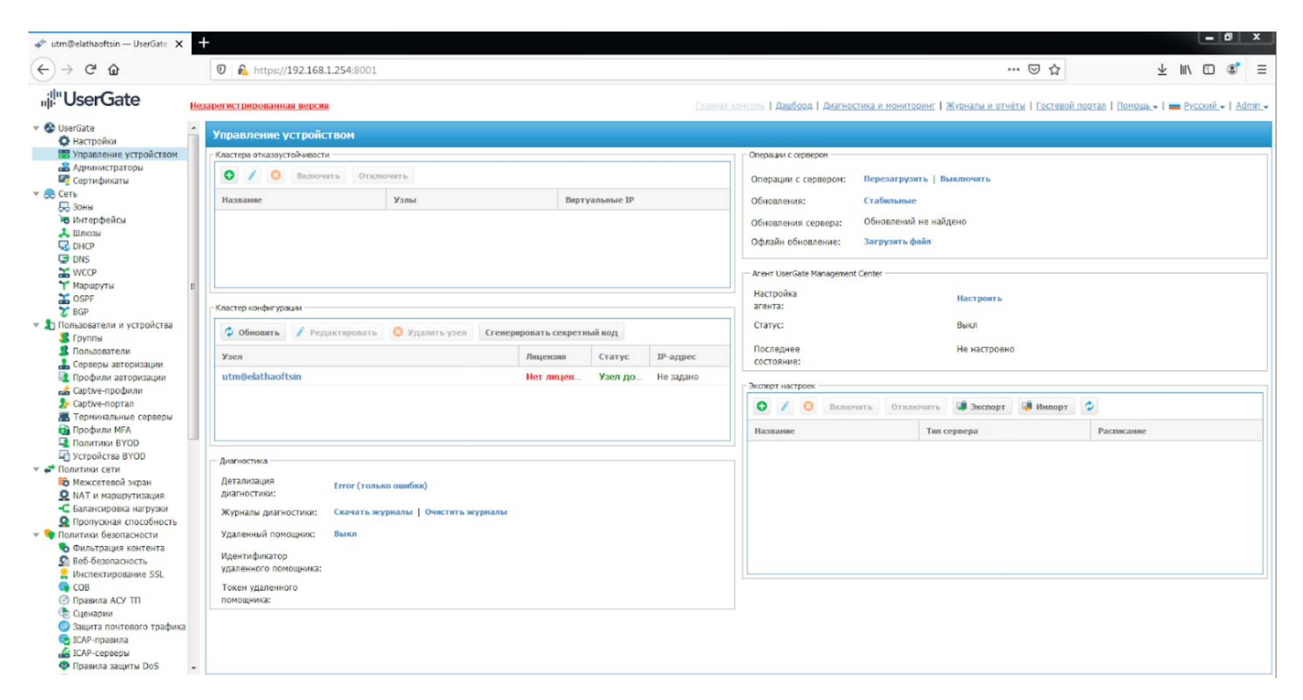


Рисунок А.5. Окно веб интерфейса управления платформой UserGate

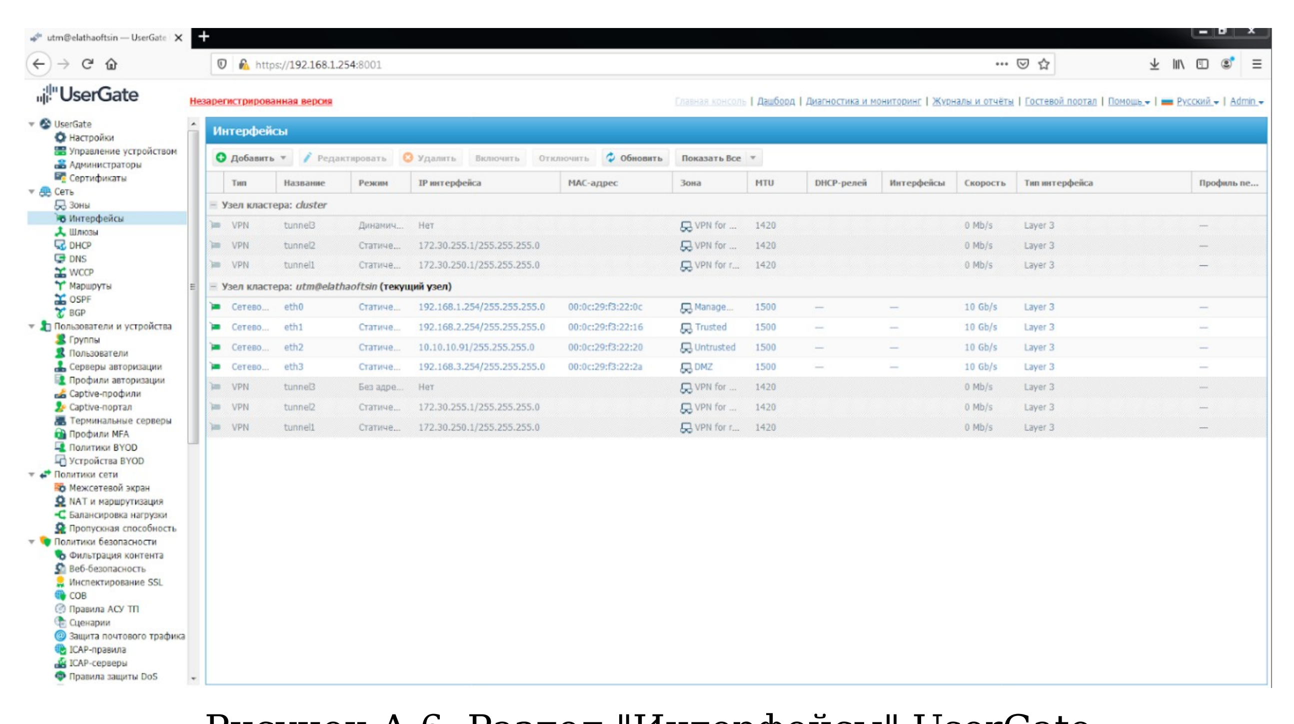


Рисунок А.6. Раздел "Интерфейсы" UserGate

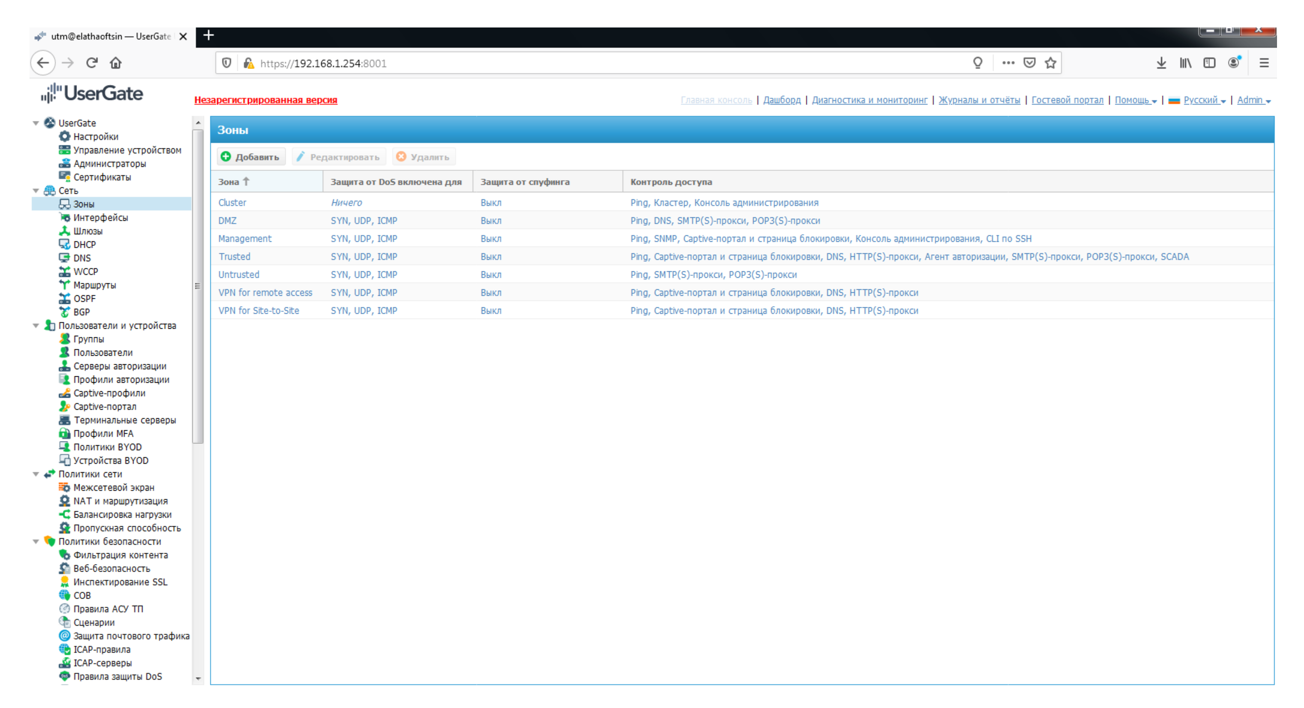


Рисунок А.7. Зоны UserGate

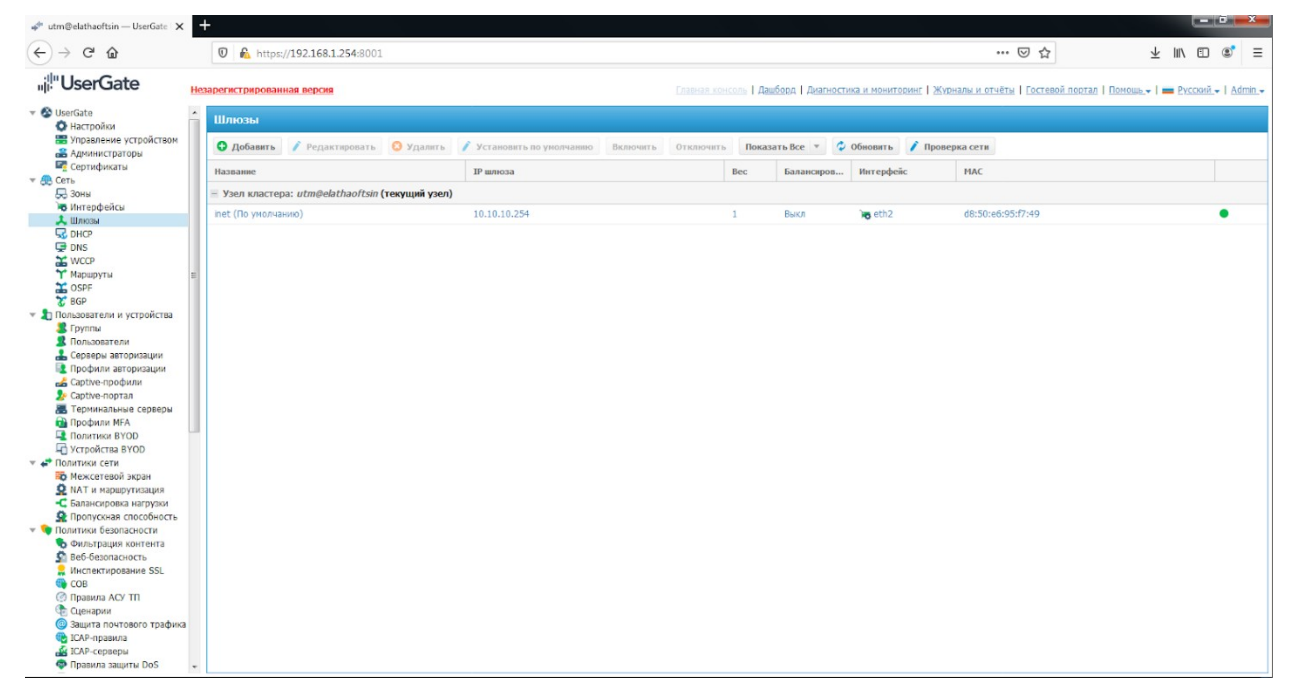


Рисунок А.8. Шлюзы UserGate

После настройки интерфейсов и маршрутов, система UserGate готова к использованию, и администратор может продолжить настройку в соответствии с требованиями и политиками безопасности организации.

В разделе "NAT и Маршрутизация" необходимо установить соответствующие правила Network Address Translation (NAT) (рисунок А.10). Для обеспечения доступа

пользователей из сети Trusted в Интернет уже создано правило NAT с названием "Trusted-->Untrusted", и остается его активировать. Важно отметить, что правила применяются в порядке сверху вниз, и выполнится только первое правило, удовлетворяющее условиям. Для срабатывания правила, все условия в его параметрах должны соответствовать. UserGate рекомендует создавать общие правила NAT, например, для передачи трафика из локальной сети (часто обозначаемой как Trusted) в Интернет, оставляя разграничение доступа по пользователям, сервисам и приложениям под управлением правил межсетевого экрана.

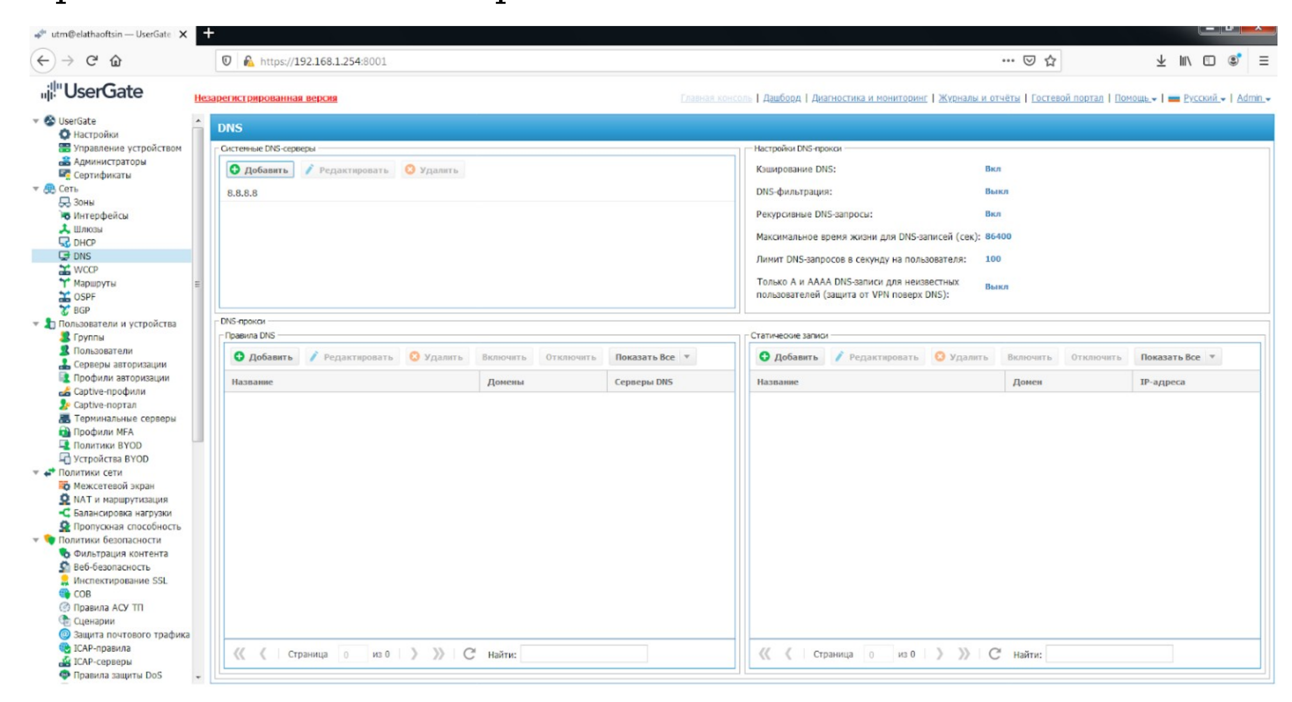


Рисунок А.9. DNS UserGate

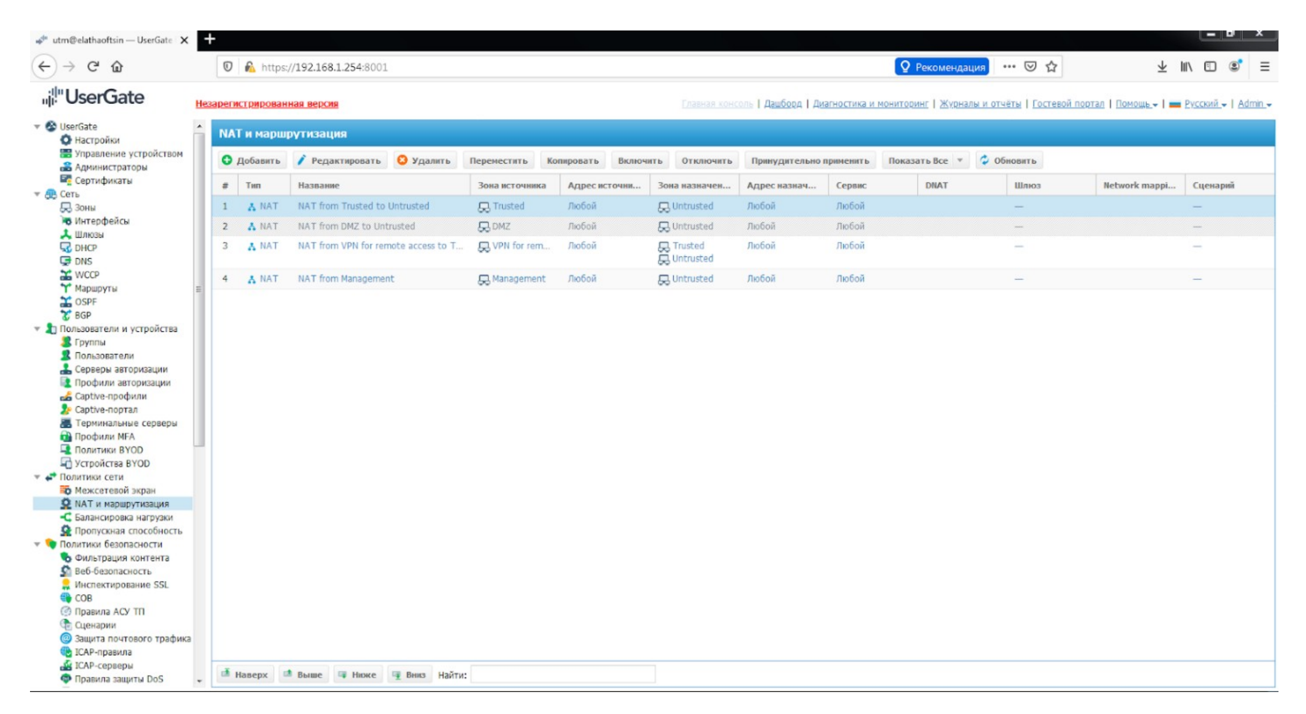


Рисунок А.10. NAT и Маршрутизация

В разделе "Межсетевой экран" требуется создать правила для обеспечения безопасности и контроля транзитного сетевого трафика (рисунок А.11). Например, правило "Internet for Trusted" уже создано для обеспечения неограниченного доступа в Интернет для пользователей сети Trusted и требует только активации. При помощи правил межсетевого экрана администратор может разрешить или запретить различные виды трафика, проходящего через UserGate. Условиями правил могут быть зоны, IP-адреса источника/назначения, пользователи, группы, а также сервисы и приложения. Правила также применяются сверху вниз, и если не создано ни одного правила, весь транзитный трафик через UserGate будет отклонен.

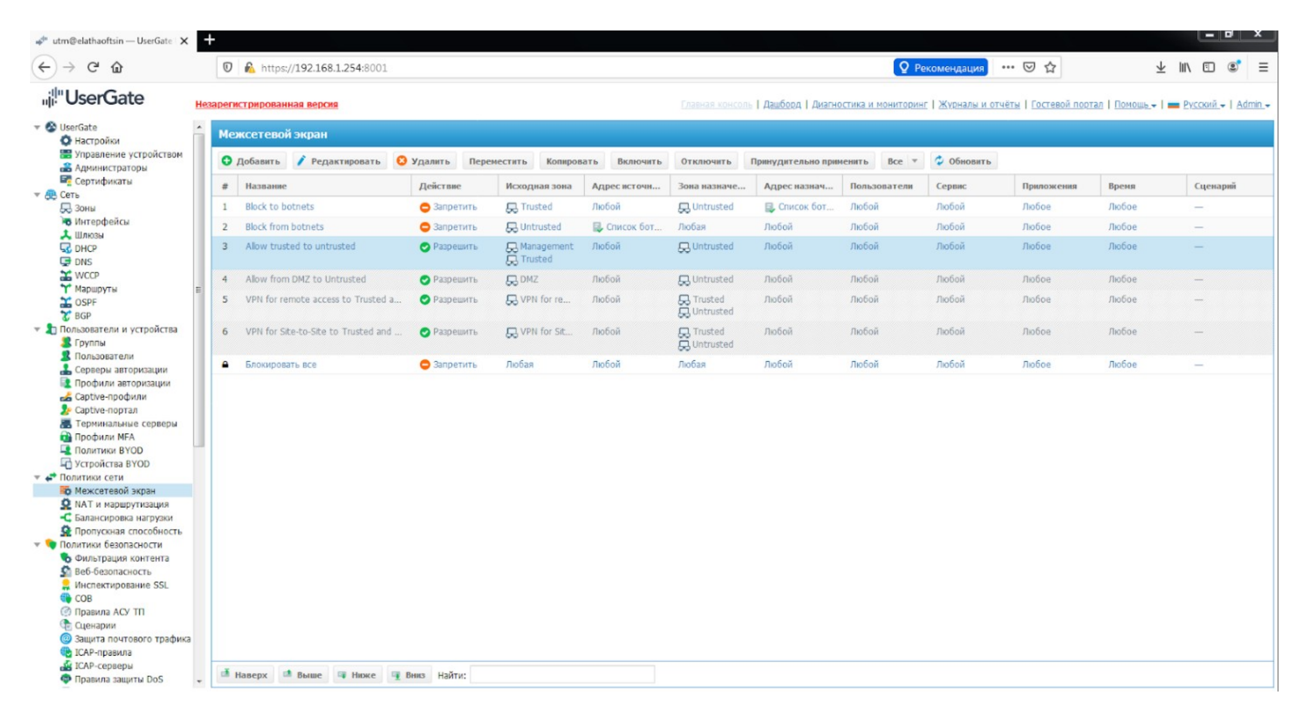


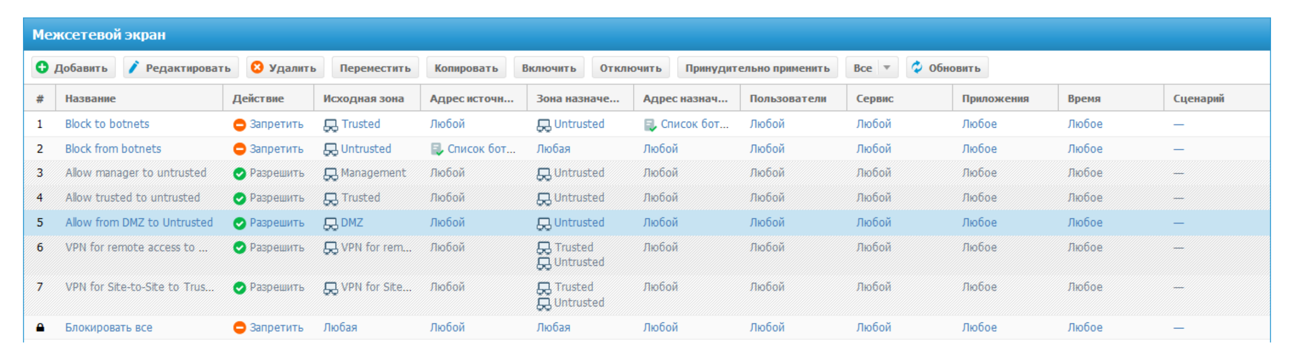
Рисунок А.11. Межсетевой экран

В разделе "NAT и Маршрутизация" создание правил подразумевает работу с различными вкладками, такими как "Межсетевой экран", "NAT и маршрутизация" и "Пропускная способность". Давайте рассмотрим более подробно, как осуществляется этот процесс.

Идеология работы правил UserGate заключается в том, что они выполняются сверху вниз до первого сработавшего. Это означает, что более специфичные правила должны находиться выше более общих в порядке выполнения. Однако следует учесть, что проверка правил происходит по порядку, поэтому в целях оптимизации рекомендуется создавать более общие правила. Условия для создания любого правила применяются согласно логике "И", и для логики "ИЛИ" можно использовать несколько правил.

После установки UserGate в разделе "Межсетевой экран" уже существует простая политика. Первые два правила блокируют трафик для бот-сетей, за которыми следуют примеры правил доступа из различных зон. Последнее

правило, обозначенное символом замка, блокирует весь неявно разрешенный трафик. Если необходимо разрешить весь трафик через UserGate (хотя это не рекомендуется), можно создать предпоследнее правило "Разрешить все" (рисунок А.12).



#	Название	Действие	Исходная зона	Адрес источн...	Зона назначе...	Адрес назнач...	Пользователи	Сервис	Приложения	Время	Сценарий
1	Block to botnets	Запретить	Trusted	Любой	Untrusted	Список бот...	Любой	Любой	Любое	Любое	—
2	Block from botnets	Запретить	Untrusted	Список бот...	Любая	Любой	Любой	Любой	Любое	Любое	—
3	Allow manager to untrusted	Разрешить	Management	Любой	Untrusted	Любой	Любой	Любой	Любое	Любое	—
4	Allow trusted to untrusted	Разрешить	Trusted	Любой	Untrusted	Любой	Любой	Любой	Любое	Любое	—
5	Allow from DMZ to Untrusted	Разрешить	DMZ	Любой	Untrusted	Любой	Любой	Любой	Любое	Любое	—
6	VPN for remote access to ...	Разрешить	VPN for rem...	Любой	Trusted Untrusted	Любой	Любой	Любой	Любое	Любое	—
7	VPN for Site-to-Site to Trus...	Разрешить	VPN for Site...	Любой	Trusted Untrusted	Любой	Любой	Любой	Любое	Любое	—
	Блокировать все	Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—

Рисунок А.12. Разрешение трафика в разделе "Межсетевой экран"

При создании правила для межсетевого экрана в разделе "Общие" следует указать:

- Включить или выключить правило.
- Название правила.
- Описание правила.
- Выбор действия: Запретить или Разрешить.
- Сценарий, который является дополнительным условием для срабатывания правила.
- Журналирование, которое записывает информацию о трафике при срабатывании правила.
- Применение правила ко всем пакетам, фрагментированным или нефрагментированным пакетам.
- Возможность выбора места в политике.

Вкладки "Источник", "Назначение", "Пользователи", "Сервис", "Приложение" и "Время" позволяют настраивать условия правила для источника, назначения, пользователей, сервиса, приложения и времени соответственно.

При создании правил NAT в разделе "Общие" появляется поле "Тип", которое позволяет выбрать между:

- NAT - Преобразование сетевых адресов.
- DNAT - Перенаправление трафика на указанный IP-адрес.
- Порт-форвардинг - Перенаправление трафика на указанный IP-адрес с возможностью изменения номера порта.
- Policy-based routing - Маршрутизация IP-пакетов на основе расширенной информации.
- Network mapping - Замена IP-адресов источника или назначения одной сети на другую.

Во всех вкладках (Источник, Назначение, Пользователи, Сервис, Приложение, Время) можно настраивать условия для правила, а в зависимости от типа NAT выбирать соответствующие параметры (рисунки А.13-А.16).

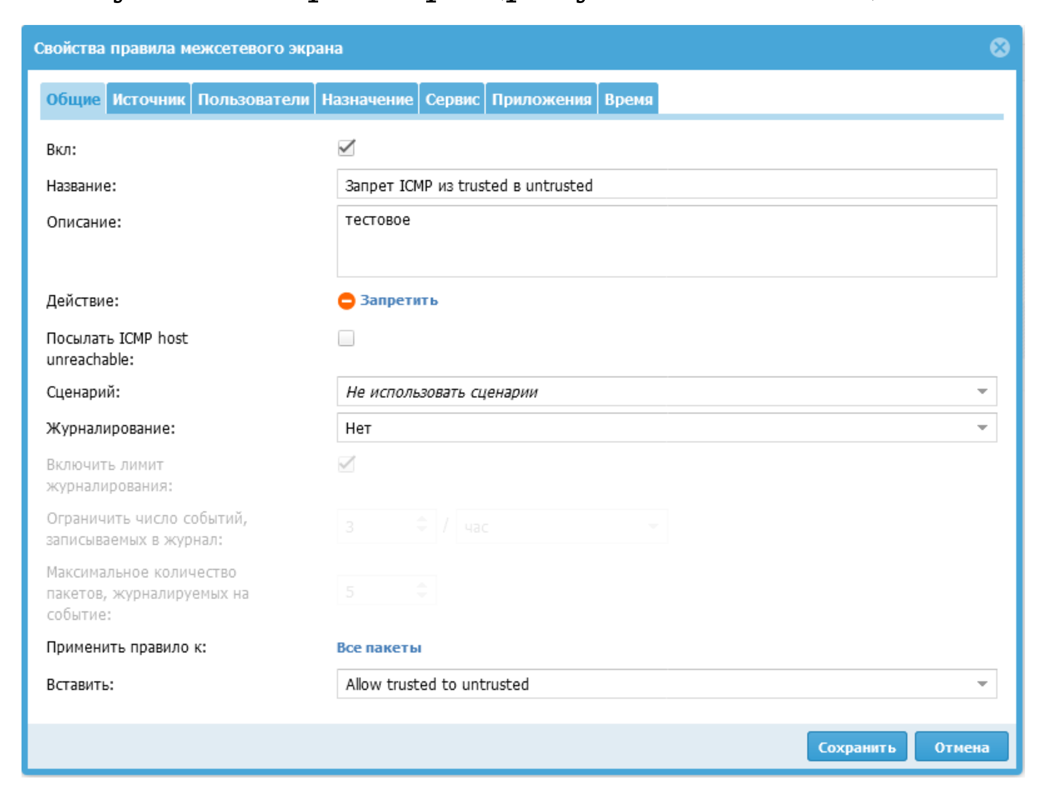


Рисунок А.13. Общие настройки правил межсетевого экрана

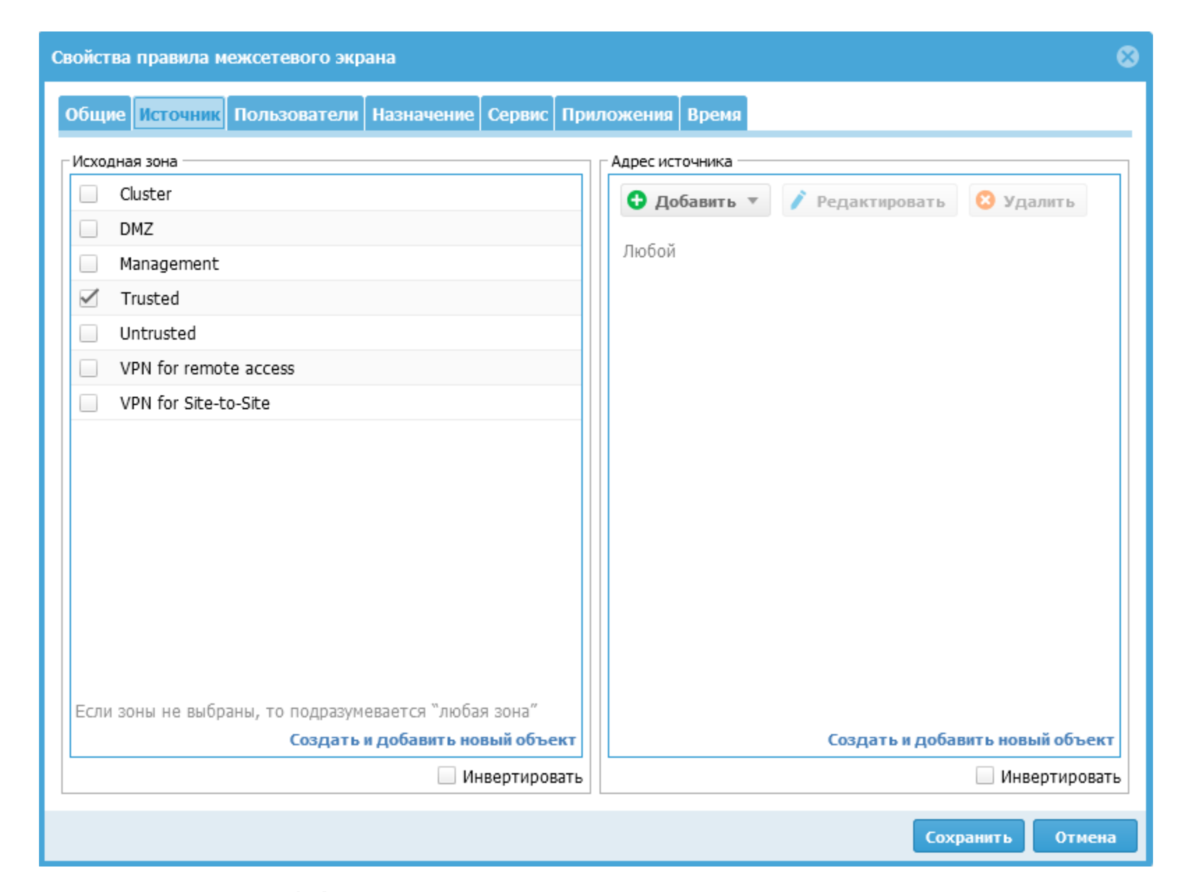


Рисунок А.14. Источник правил межсетевого экрана

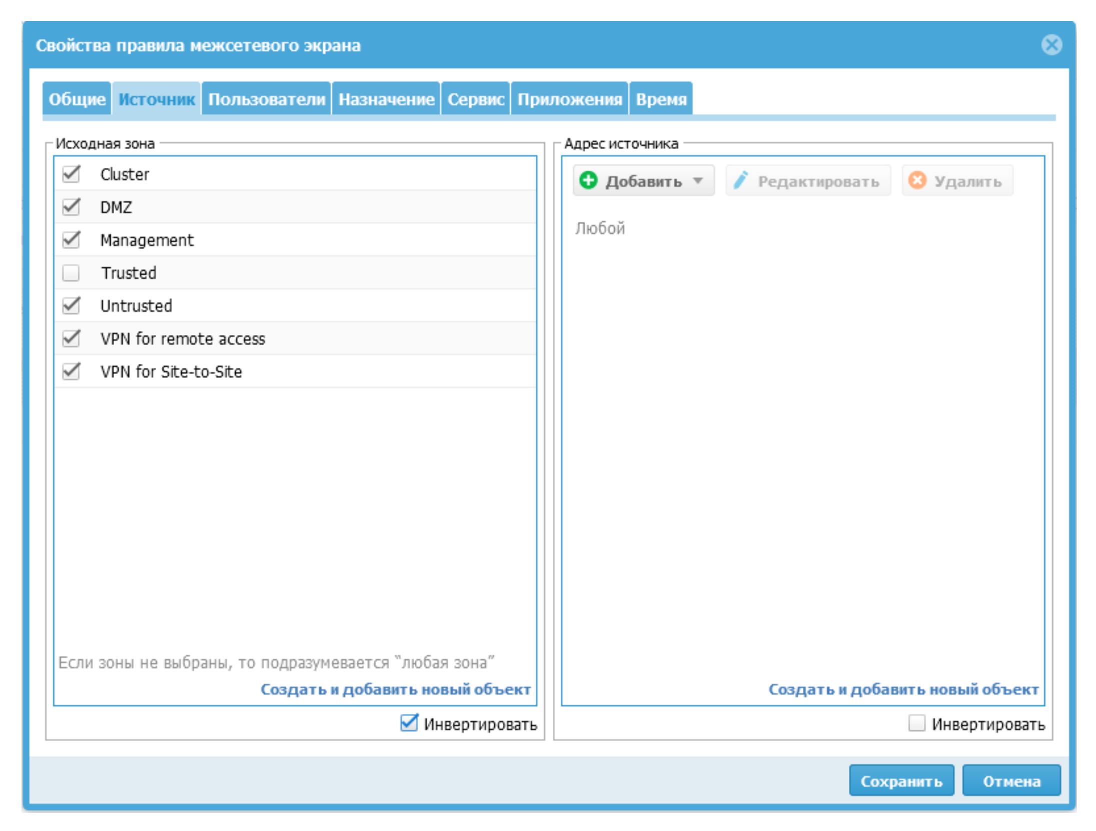


Рисунок А.15. Настройки источника правил межсетевого экрана

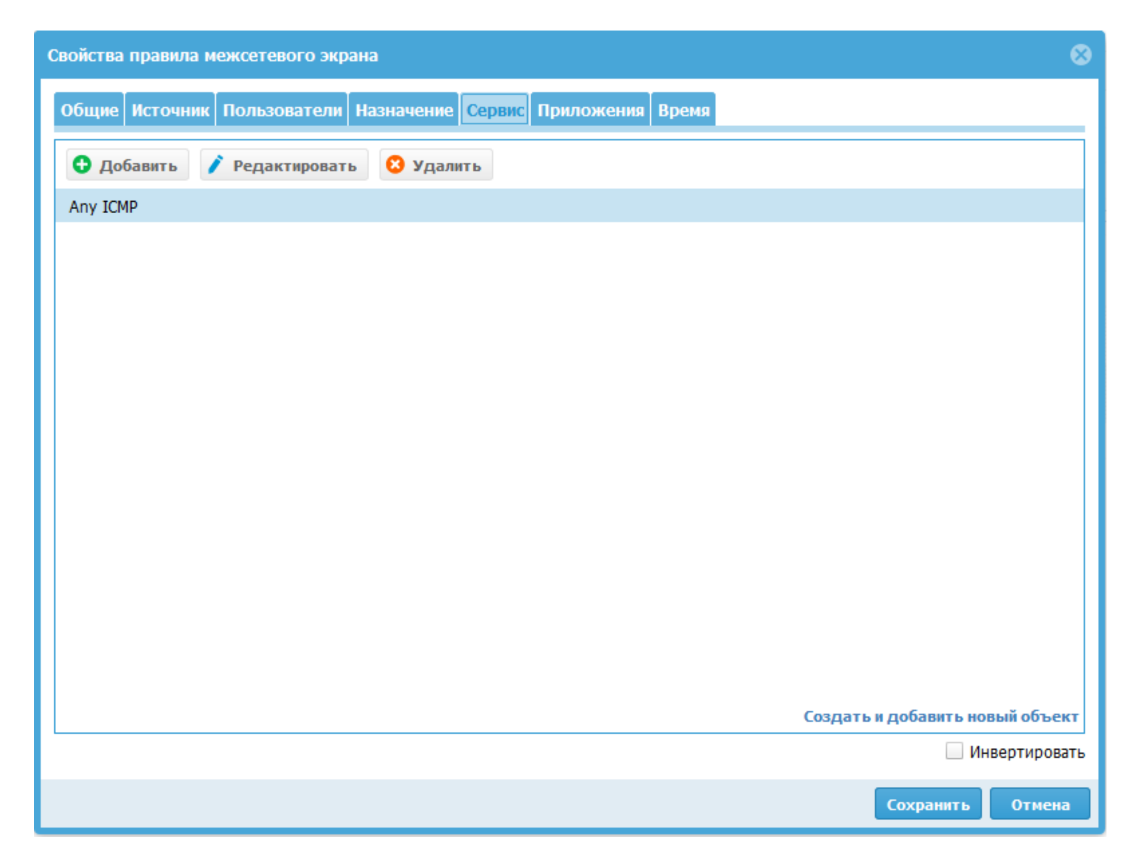


Рисунок А.16. Сервис правил межсетевого экрана

Таким образом, UserGate предоставляет гибкие инструменты для создания правил межсетевого экрана и NAT, позволяя администраторам тщательно настраивать безопасность и маршрутизацию трафика в сети.

После выбора соответствующего типа правила, необходимо настроить его параметры. В поле "SNAT IP" (внешний адрес) указывается явный IP-адрес, который заменит адрес источника. Это поле становится важным при наличии нескольких IP-адресов на интерфейсах зоны назначения. Рекомендуется явно указывать SNAT IP для повышения производительности межсетевого экрана. Если оставить поле пустым, система будет использовать произвольный адрес из доступных IP-адресов.

Приведем пример настройки порт-форвардинга (*Port Forwarding*): для публикации SSH сервиса сервера Windows, находящегося в зоне "DMZ". Создаем правило "SSH to

Windows" с типом "Порт-форвардинг" (рисунок А.17). В разделе "Источник" выбираем зону "Untrusted". На вкладке "Порт-форвардинг" указываем протокол (TCP), оригинальный порт назначения (9922) и новый порт назначения (22), на который будет пересылаться трафик (рисунок А.18).

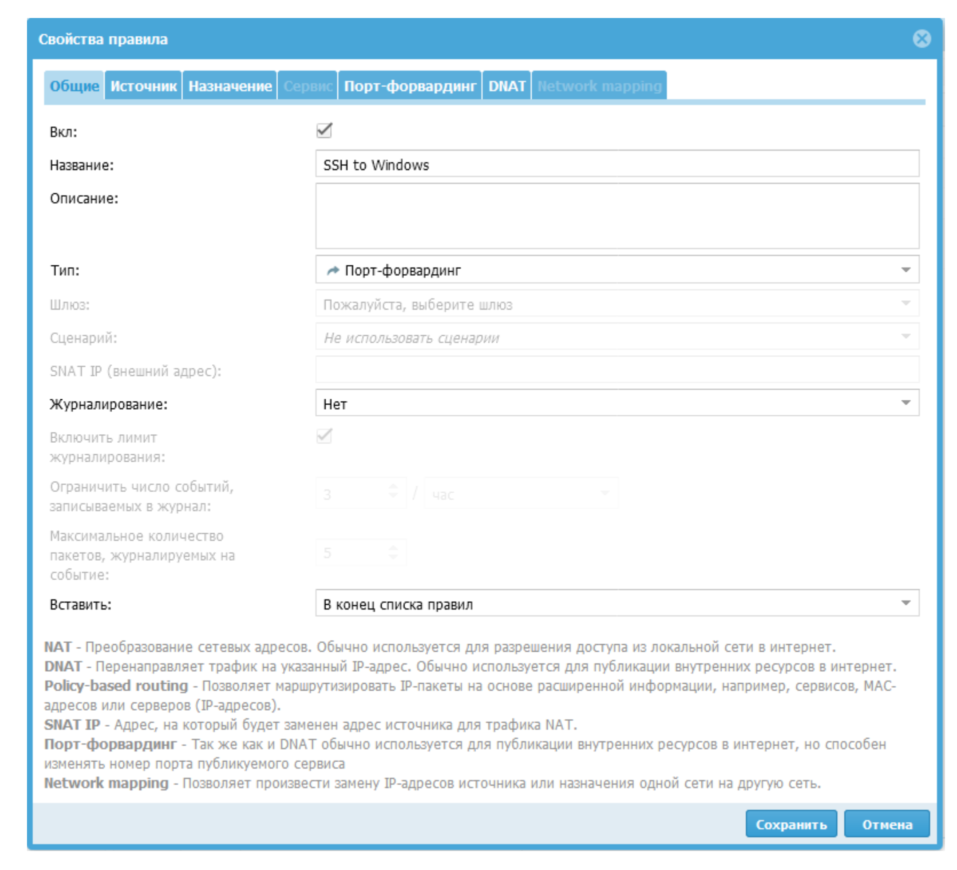


Рисунок А.17. Публикация SSH сервиса сервера Windows

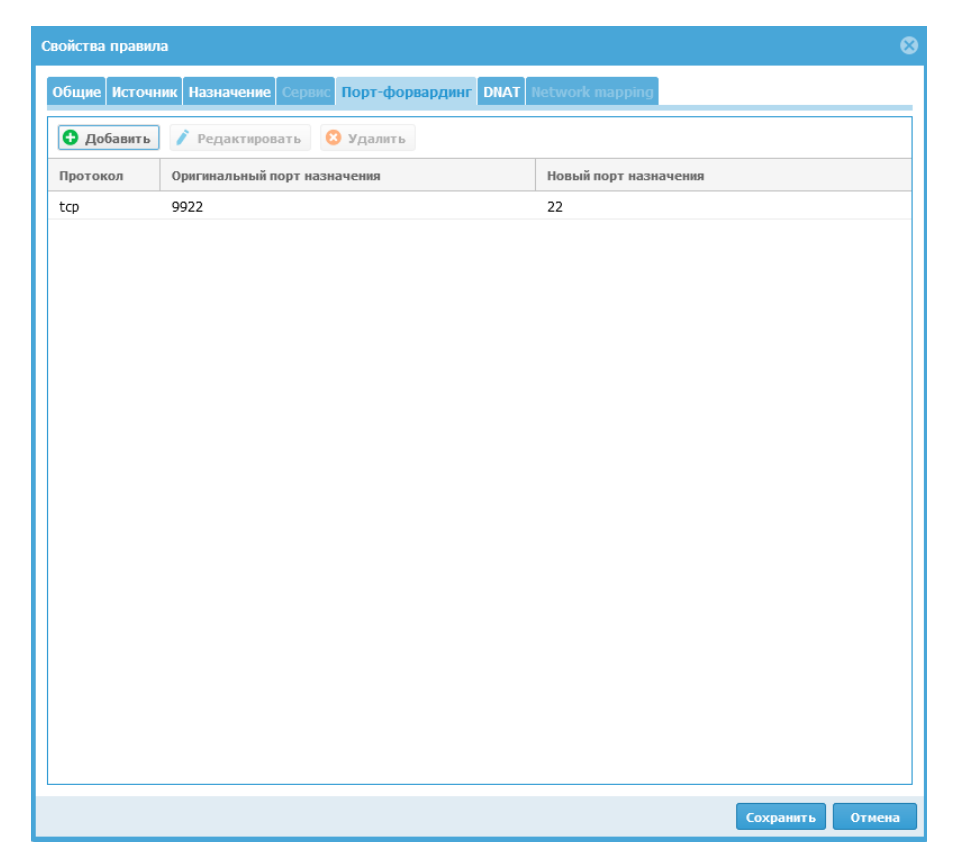


Рисунок А.18. Настройка Порт-форвардинга

Далее, на вкладке "DNAT", задаем IP-адрес компьютера в локальной сети (192.168.3.2), который будет публиковаться в интернете. Опционально можно включить SNAT, чтобы UserGate изменял адрес источника в пакетах из внешней сети на свой IP-адрес (рисунок А.19).

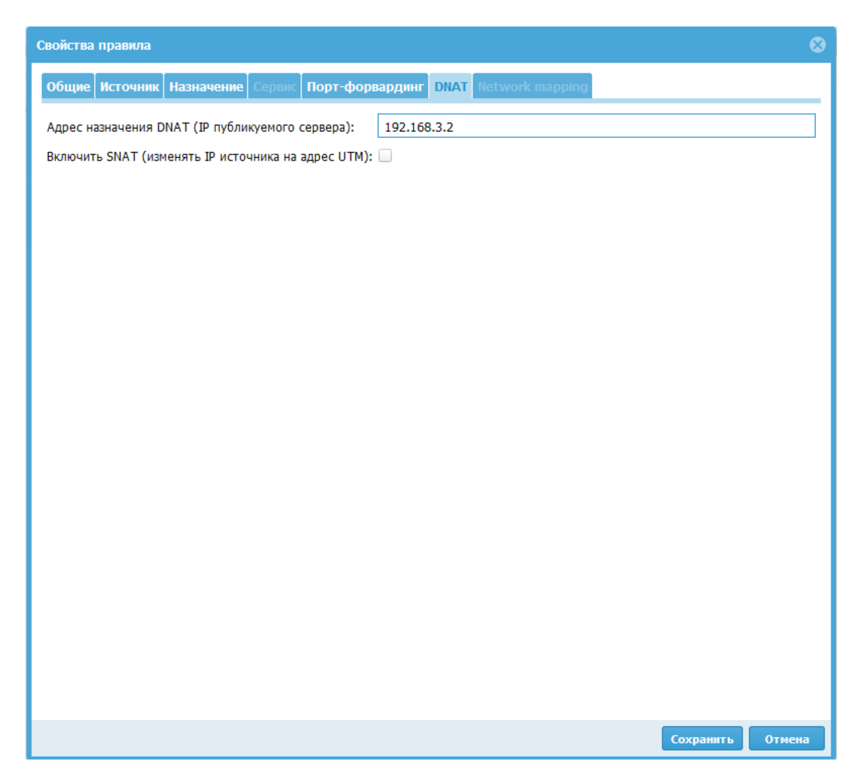
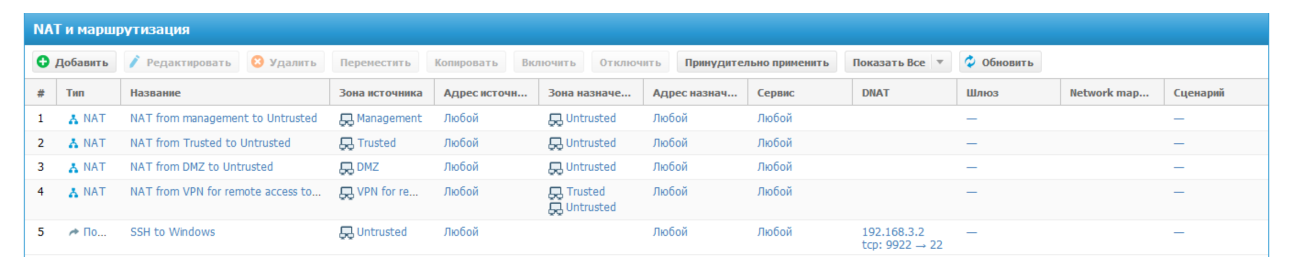


Рисунок А.19. Настройка DNAT

Таким образом, создается правило, позволяющее получить доступ из зоны "Untrusted" к серверу с IP-адресом 192.168.3.2 по протоколу SSH, используя внешний адрес UserGate (рисунок А.20).



#	Тип	Название	Зона источника	Адрес источн...	Зона назначе...	Адрес назнач...	Сервис	DNAT	Шлюз	Network map...	Сценарий
1	NAT	NAT from management to Untrusted	Management	Любой	Untrusted	Любой	Любой		—		—
2	NAT	NAT from Trusted to Untrusted	Trusted	Любой	Untrusted	Любой	Любой		—		—
3	NAT	NAT from DMZ to Untrusted	DMZ	Любой	Untrusted	Любой	Любой		—		—
4	NAT	NAT from VPN for remote access to...	VPN for re...	Любой	Trusted Untrusted	Любой	Любой		—		—
5	По...	SSH to Windows	Untrusted	Любой		Любой	Любой	192.168.3.2 tcp: 9922 → 22	—		—

Рисунок А.20. Просмотр результатов настройки NAT и маршрутизации

В разделе "Пропускная способность" настраиваются правила для управления пропускной способностью. Они могут ограничивать канал для определенных пользователей, хостов, сервисов и приложений (рисунок А.21).

При создании правила на вкладках определяются условия применения ограничений. Полосу пропускания можно выбрать из предложенных или задать свою (рисунок

А.22). Метку приоритезации трафика DSCP можно указать при создании полосы пропускания. Например, сценарий в правиле может автоматически изменить метки DSCP. Другой пример использования сценария: правило сработает для пользователя только при обнаружении торрента или если объем трафика превысит заданный предел.

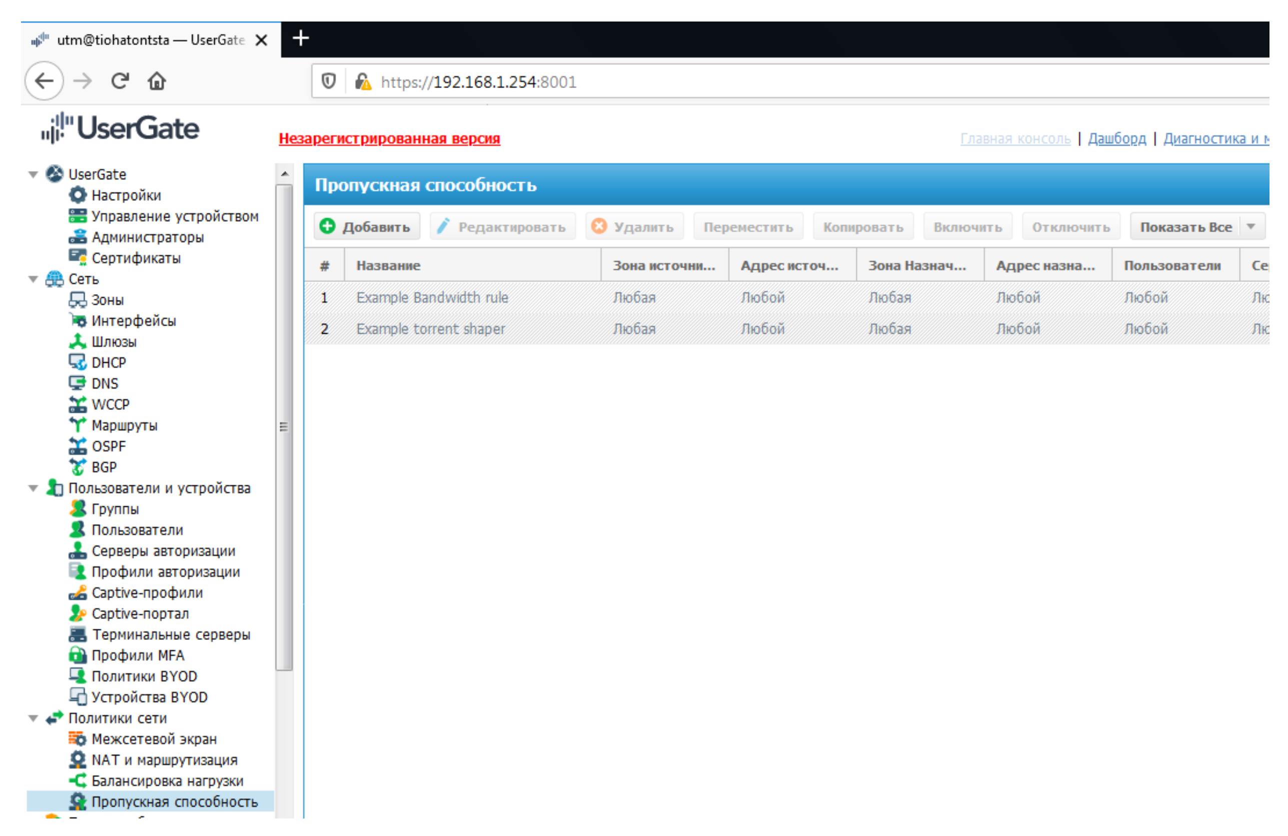


Рисунок А.21. Раздел "Пропускная способность"

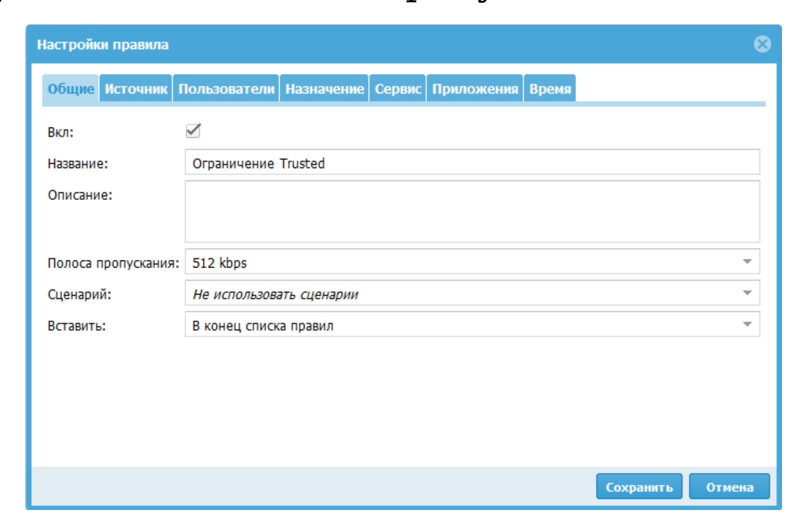


Рисунок А.22. Настройки правил пропускной способности

Остальные вкладки заполняются аналогично другим

политикам, в зависимости от типа трафика, к которому применяется правило.

Приложение Б. Анализ работы системы межсетевого экранирования в компании

Идентификация пользователей в UserGate позволяет точечно применять политики безопасности и правила межсетевого экрана. UserGate оперирует четырьмя типами пользователей: Unknown, Known, Any, и Определенный пользователь. Идентификация может происходить через различные методы, такие как логин и пароль, IP/MAC-адреса, VLAN ID или даже методы прозрачной идентификации, например, через Kerberos.

При создании локальных пользователей необходимо указать их имя, логин и пароль. Дополнительно можно задать IP-адрес, MAC-адрес или VLAN ID для идентификации пользователя. Электронные почтовые адреса и номера телефонов могут быть добавлены для отправки информации пользователю. При наличии логина, пароля и адреса, система использует идентификацию по адресу, приоритетнее по сравнению с другими методами (рисунки Б.1, Б.2).

Для более удобного управления политиками безопасности, пользователи могут быть объединены в группы (рисунок Б.3).

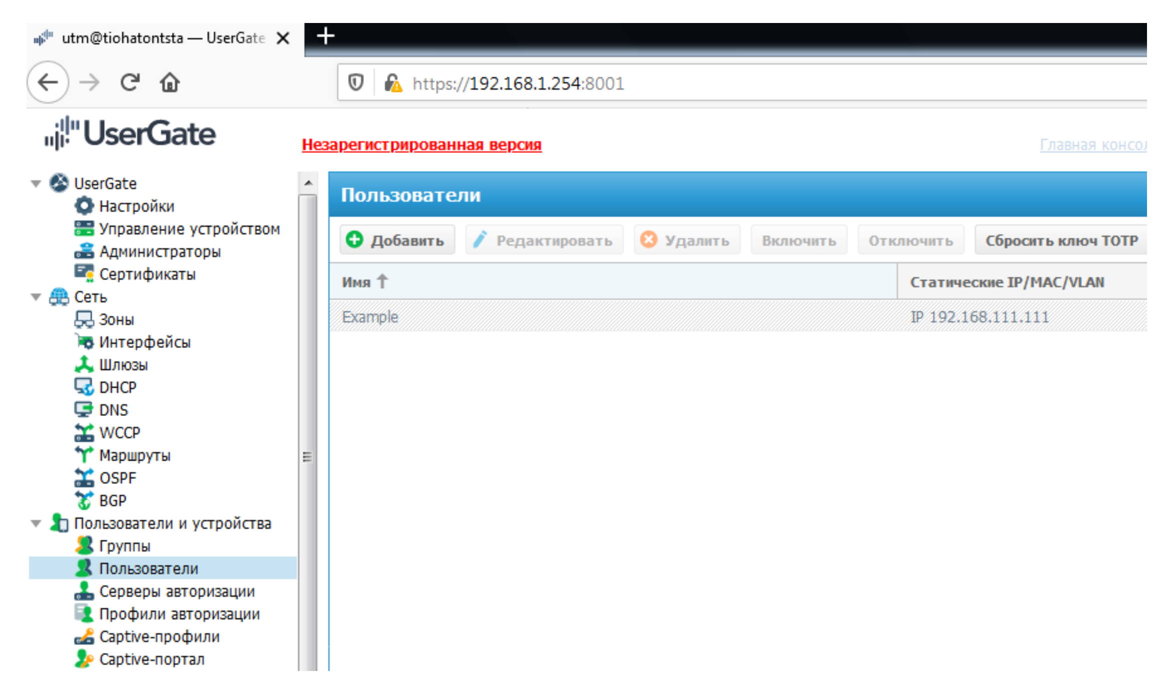


Рисунок Б.1. Раздел пользователей

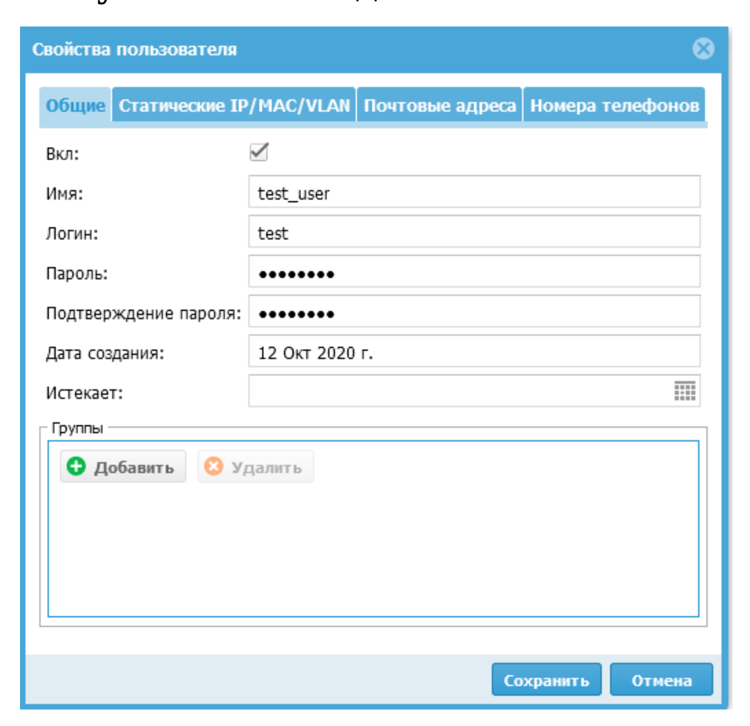


Рисунок Б.2. Свойства пользователя

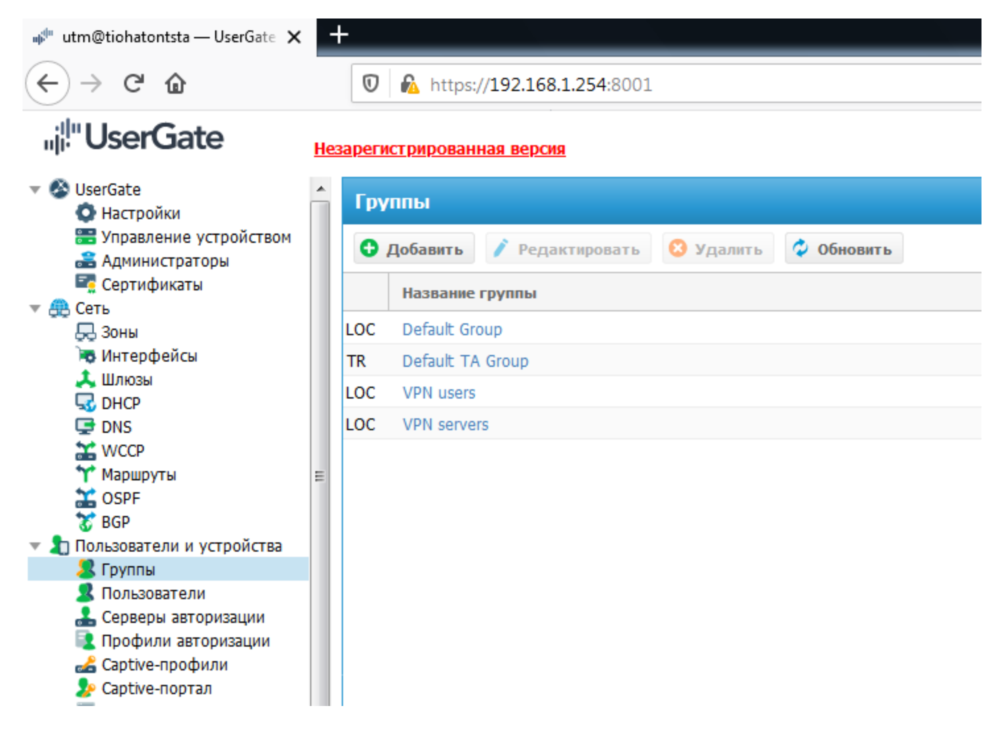


Рисунок Б.3. Создание групп

LDAP-коннектор позволяет UserGate подключаться к Active Directory. При создании коннектора указываются доменное имя LDAP или IP-адрес сервера, а также учетные данные для подключения. Дополнительно, можно указать путь поиска для сужения области поиска пользователей и групп. Кроме того, можно загрузить Kerberos keytab-файл для снижения нагрузки на серверы LDAP (рисунки Б.4, Б.5).

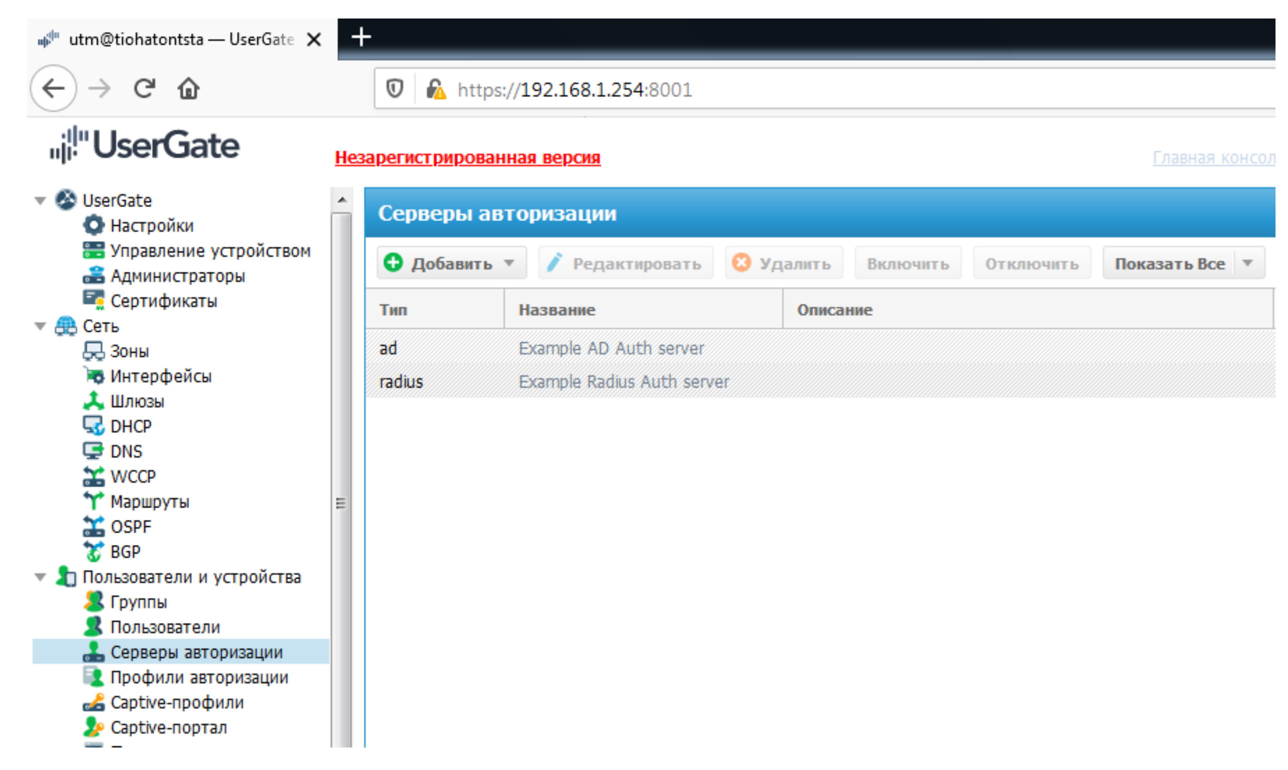


Рисунок Б.4. Серверы авторизации

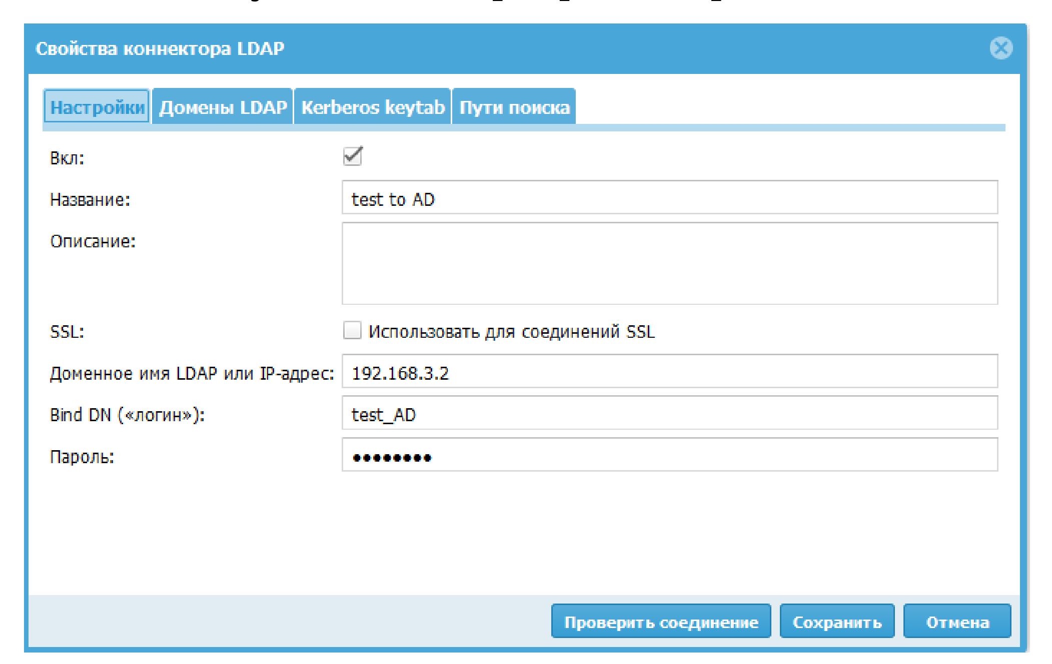


Рисунок Б.5. Настройки свойств коннектора

Captive-портал в UserGate используется для авторизации пользователей, особенно для тех, кто не был идентифицирован другими методами. Он поддерживает авторизацию только для протоколов HTTP и HTTPS. Для этого создаются профили авторизации и captive-профили (рисунок Б.6).

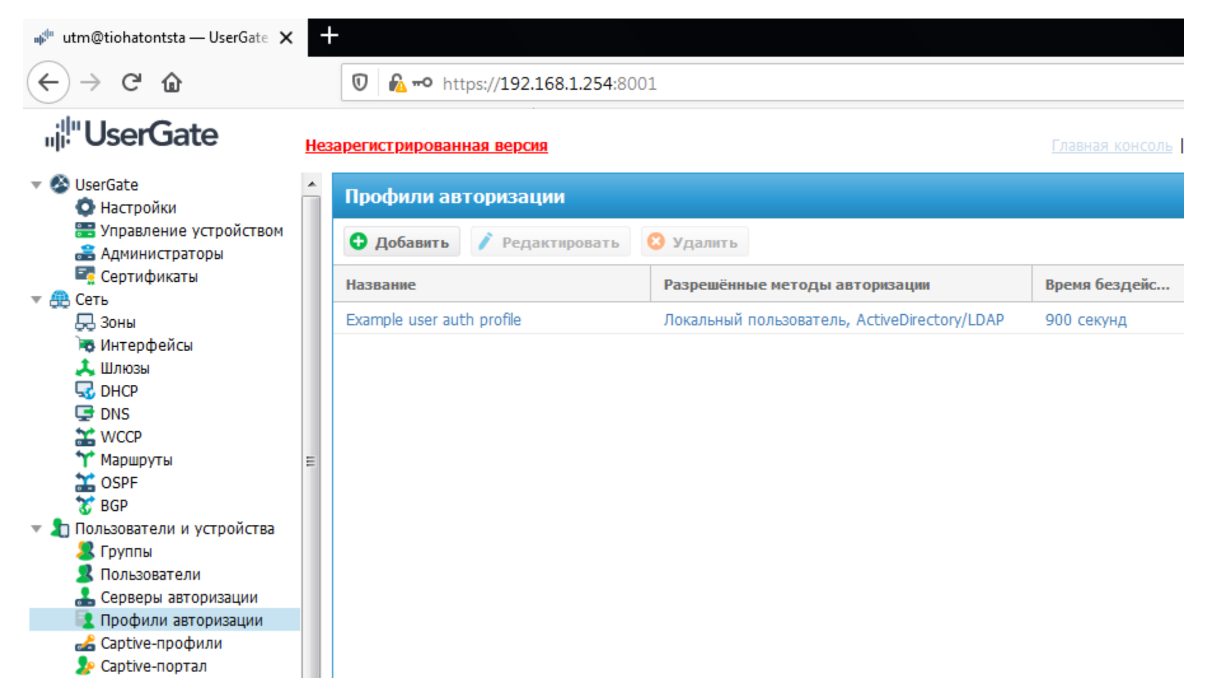


Рисунок Б.6. Добавление профиля авторизации

Captive-профиль определяет условия и методы идентификации. В процессе идентификации, можно запоминать IP-адрес или использовать cookie в браузере пользователя (рисунок Б.7, Б.8). С помощью Captive-портала можно настроить самостоятельную регистрацию пользователей с подтверждением идентификации через SMS или e-mail. (рисунки Б.9- Б.11).

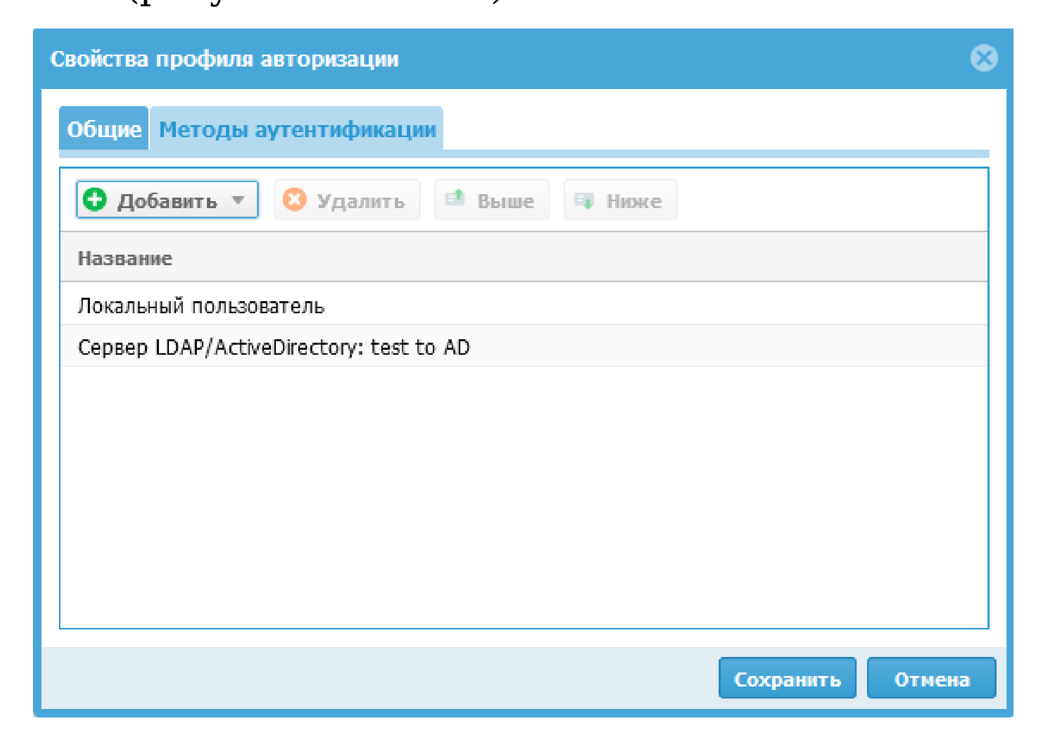


Рисунок Б.7. Указание условия и метода идентификации

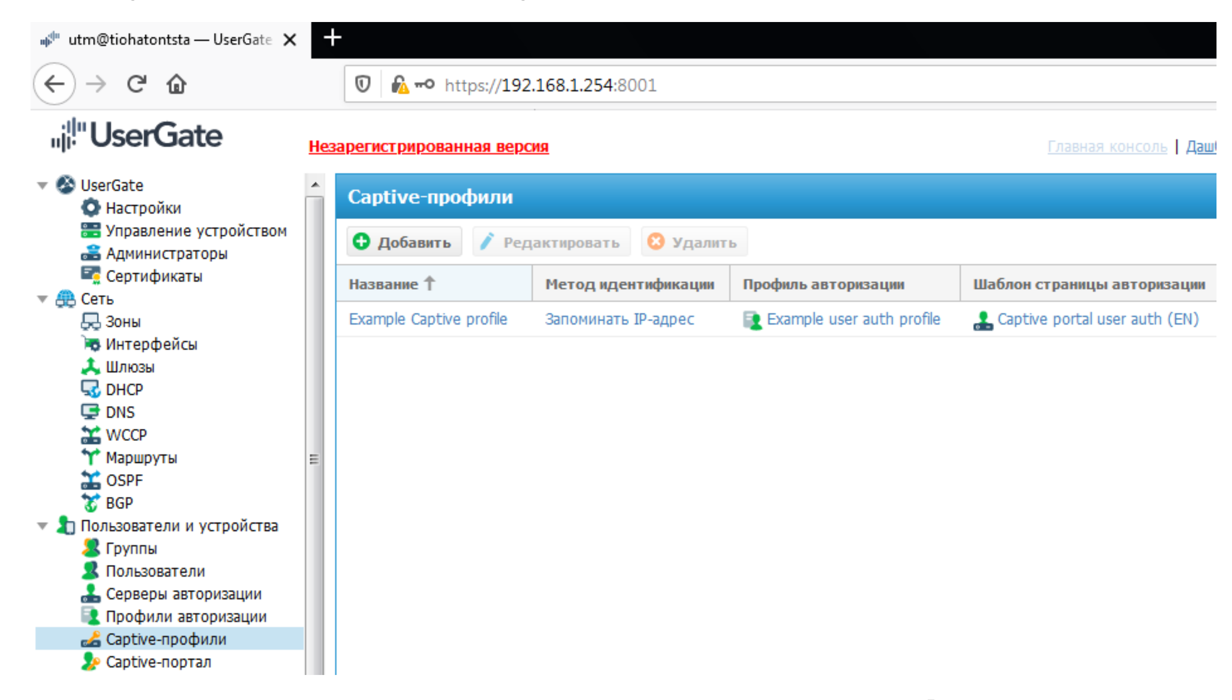


Рисунок Б.8. Создание Captive-профиля

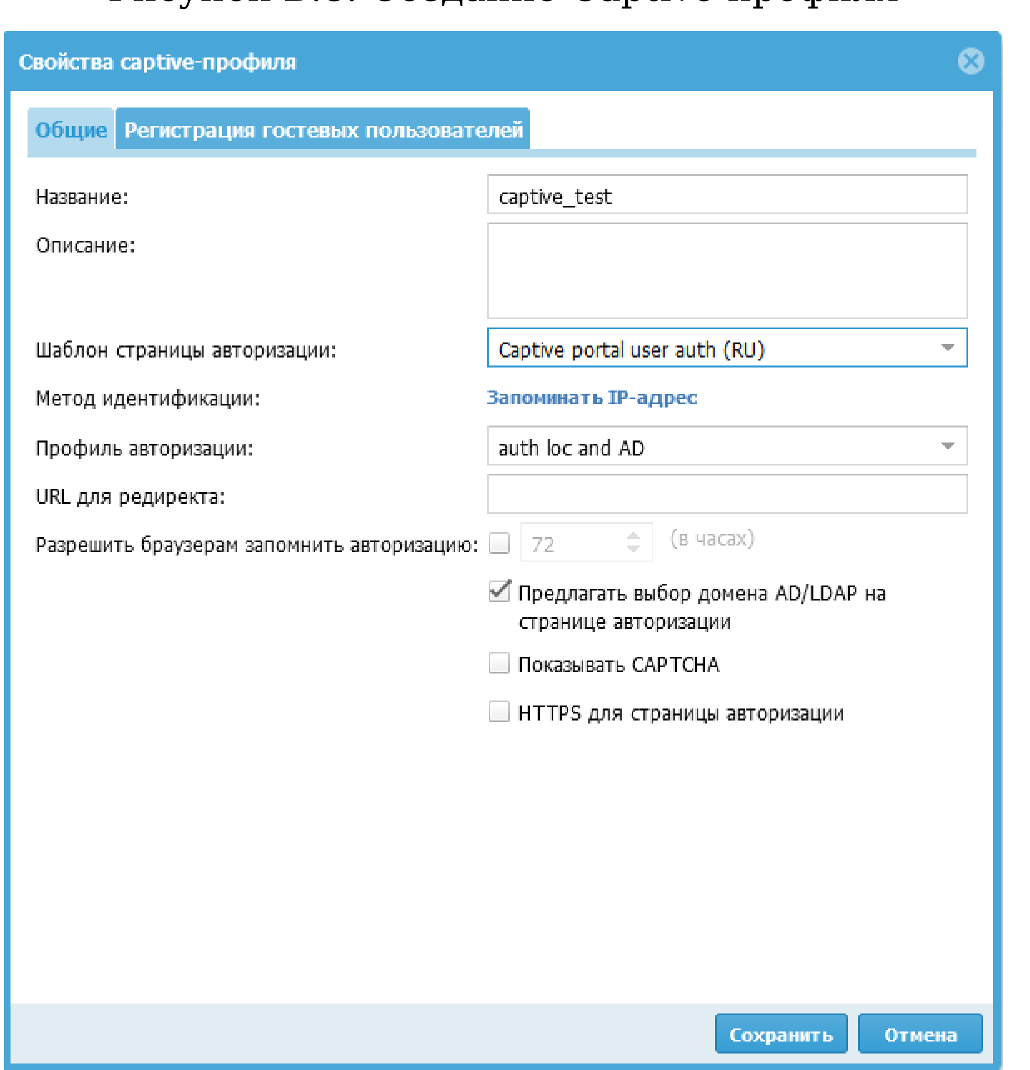


Рисунок Б.9. Указание свойств Captive-профиля

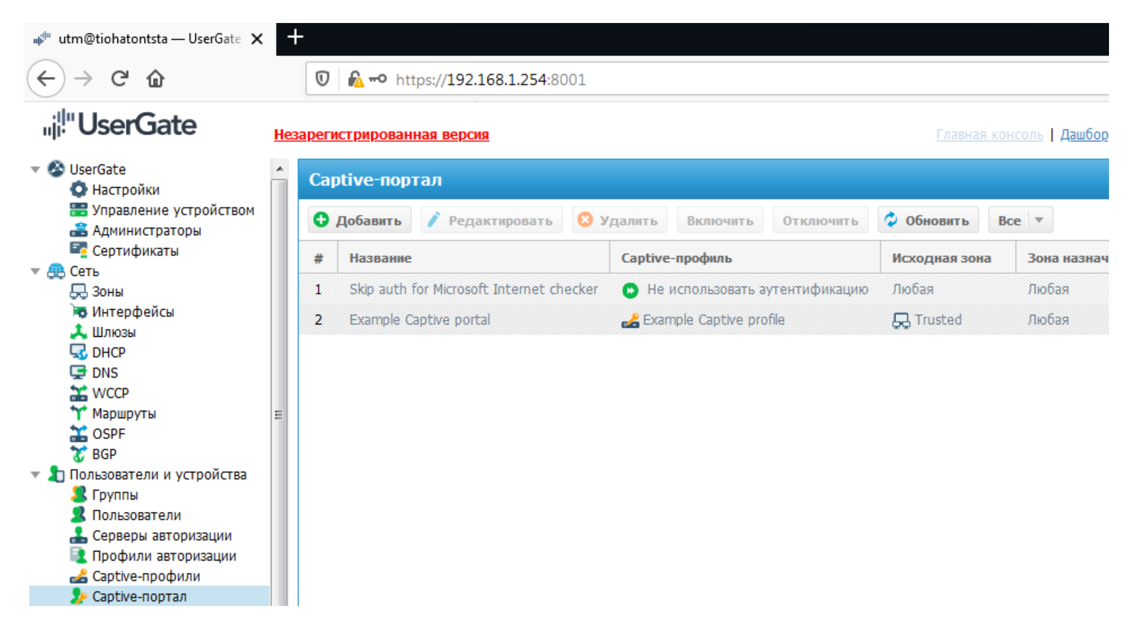


Рисунок Б.10. Создание правила в Captive-портале

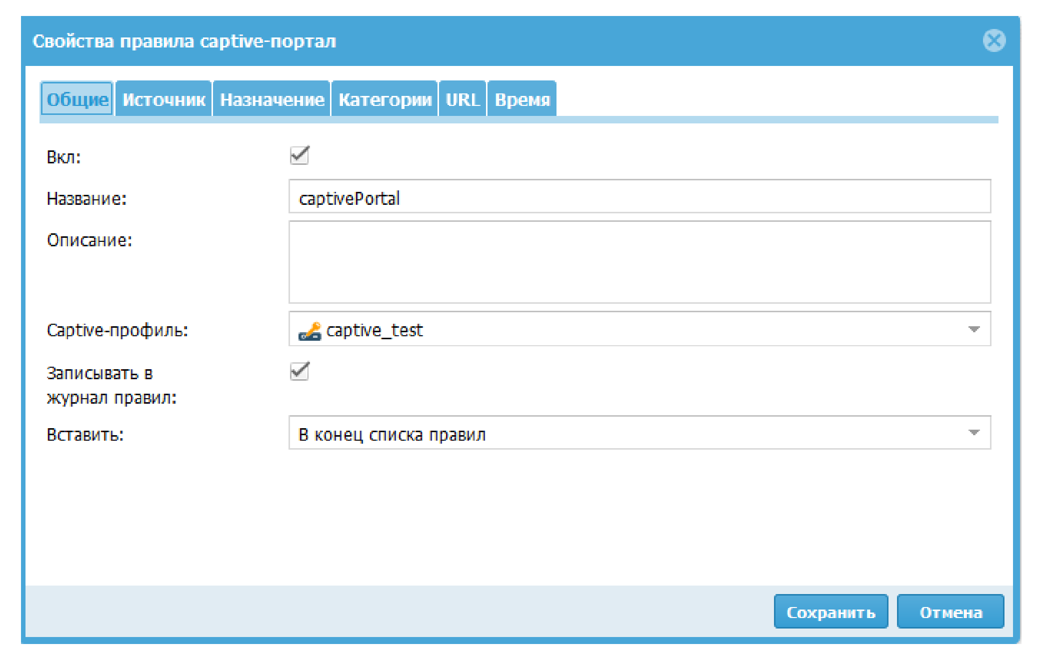


Рисунок Б.11. Задание свойств правила Captive-портала

Инспектирование SSL в UserGate базируется на технологии атаки man-in-the-middle. Это означает, что устройство проводит атаку, становясь посредником между клиентом и сервером. Для этой атаки требуется subordinate certificate CA, используемый для генерации SSL-сертификатов интернет-хостов. UserGate поставляется с набором сертификатов, включая CA (Default) - самоподписанный сертификат для инспекции SSL.

Сертификат можно скачать по прямой ссылке с шлюза: http://UserGate_IP:8002/cps/ca (рисунок Б.12).

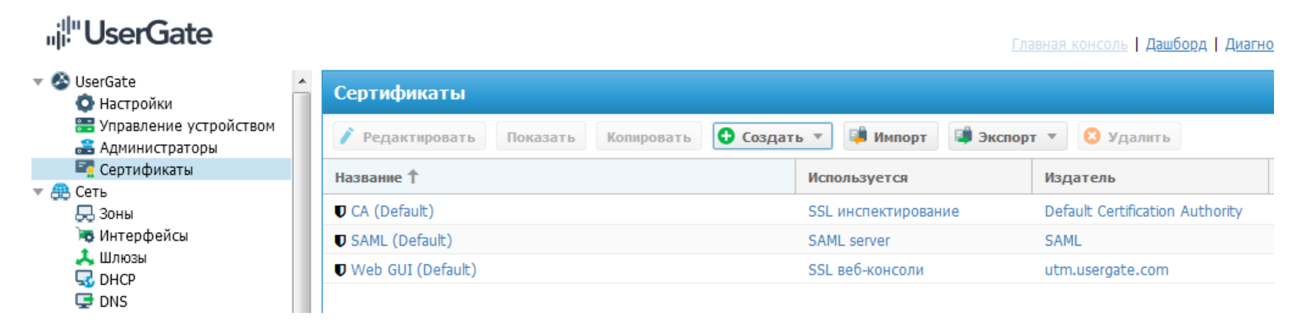


Рисунок Б.12. Сертификаты SSL

Настройка Инспектирования SSL (рисунок Б.13):

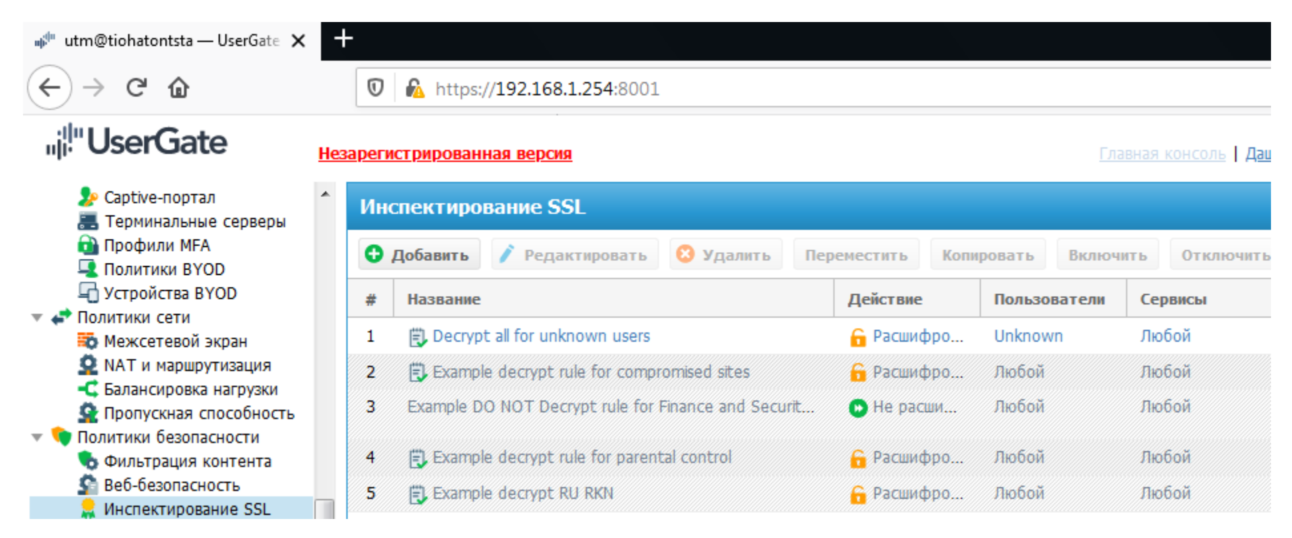


Рисунок Б.13. Раздел Инспектирование SSL

1. Создание Правила (рисунок Б.14):

- Создайте новое правило и на вкладке "Общие" определите, что делать при совпадении всех условий. Действие может быть "расшифровать" или "не расшифровать".

- Добавьте дополнительные условия, такие как блокировка сайтов с некорректными сертификатами, проверка по списку отозванных сертификатов, блокировка истекших и самоподписанных сертификатов.

2. Дополнительные Настройки:

- Настройте вкладки "Пользователи", "Источник" (зона "Trusted") и "Адрес назначения" (указание списков IP-

адресов назначения трафика) согласно предыдущим статьям.

- На вкладке "Сервис" выберите тип трафика, такой как HTTPS, SMTPS, POP3S.
- Во вкладке "Категории" можно указать конкретную категорию сайтов, а не хост. Здесь также можно проверить к какой категории принадлежит сайт (рисунок Б.15).

3. Настройка Доменов:

- В разделе "Домены" укажите список сайтов, используя только доменные имена (например, www.example.com, а не http://www.example.com/home/).

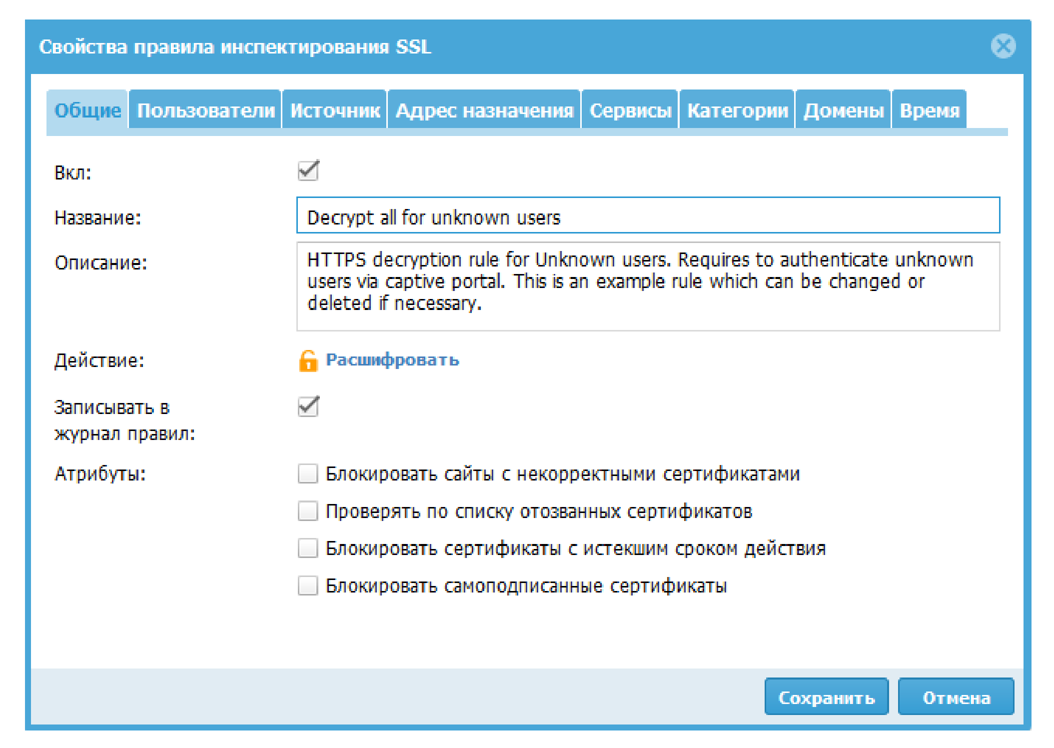


Рисунок Б.14. Настройка инспектирования SSL

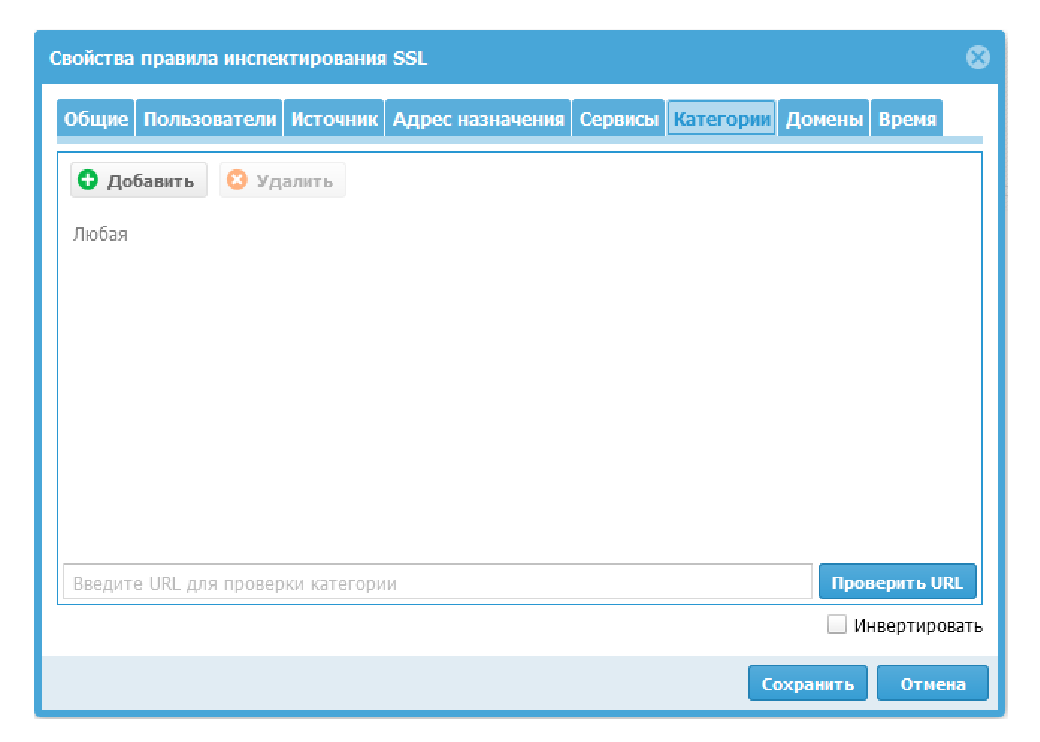
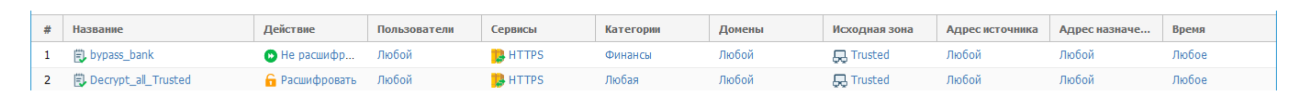


Рисунок Б.15. Добавление категории сайтов

Пример Создания Правила (рисунок Б.16):

Для исключения инспекции SSL для сайтов, связанных с финансами, создадим правило "bypassbank":

- Название правила: "bypassbank"
- Действие: "Не расшифровывать"
- Расположение: "В начало списка правил"
- Вкладка "Источник": Зона "Trusted"
- Вкладка "Сервисы": "HTTPS"
- Вкладка "Категории": Добавить категорию "Финансы"



#	Название	Действие	Пользователи	Сервисы	Категории	Домены	Исходная зона	Адрес источника	Адрес назначе...	Время
1	bypass_bank	Не расшифр...	Любой	HTTPS	Финансы	Любой	Trusted	Любой	Любой	Любое
2	Decrypt_all_Trusted	Расшифровать	Любой	HTTPS	Любая	Любой	Trusted	Любой	Любой	Любое

Рисунок Б.16. Результаты инспектирования SSL

Таким образом, пропускаем трафик к сайтам категории "Финансы", не проводя SSL-инспекцию, и затем дешифруем остальной трафик. Если нет созданных правил в политике SSL инспекции, SSL не перехватывается, и контент, передаваемый по SSL, не фильтруется.

Рассмотрим раздел "Политики безопасности", сосредоточившись на функции "Фильтрация контента" в системе UserGate. Этот инструмент позволяет администратору управлять доступом к определенному контенту, передаваемому по протоколам HTTP и HTTPS (при условии включенного инспектирования HTTPS) (рисунок Б.17).

Правила фильтрации контента в UserGate применяются сверху вниз, и первое сработавшее правило определяет дальнейшую обработку трафика. В конце списка находится правило "Разрешить все", которое нельзя удалить или изменить. Если трафик не соответствует другим правилам, он будет автоматически разрешен (рисунок Б.18).

Дополнительные вкладки в правилах фильтрации контента:

1. Тип контента:

- Выбор типов контента, предоставленных UserGate. Эти списки нельзя редактировать, но их можно использовать в правилах. Можно также создать собственные списки, добавив нужный MIME-тип (например, application/zip).

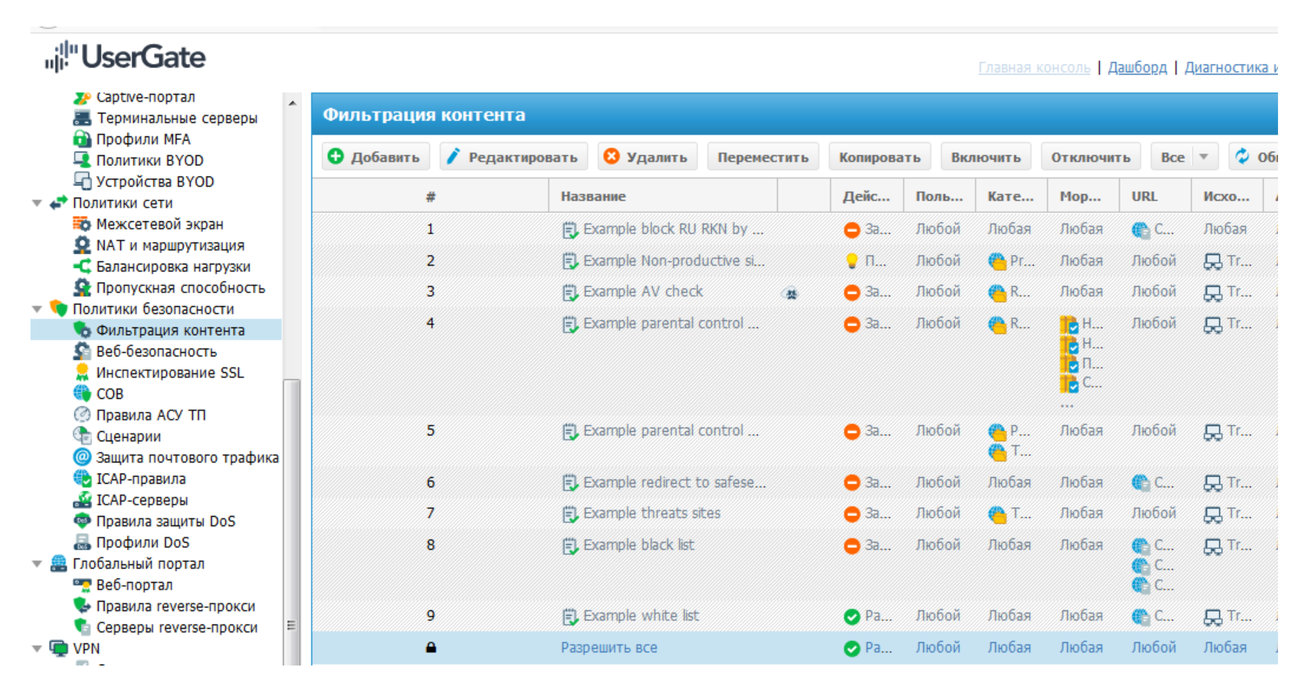


Рисунок Б.17. Фильтрация контента

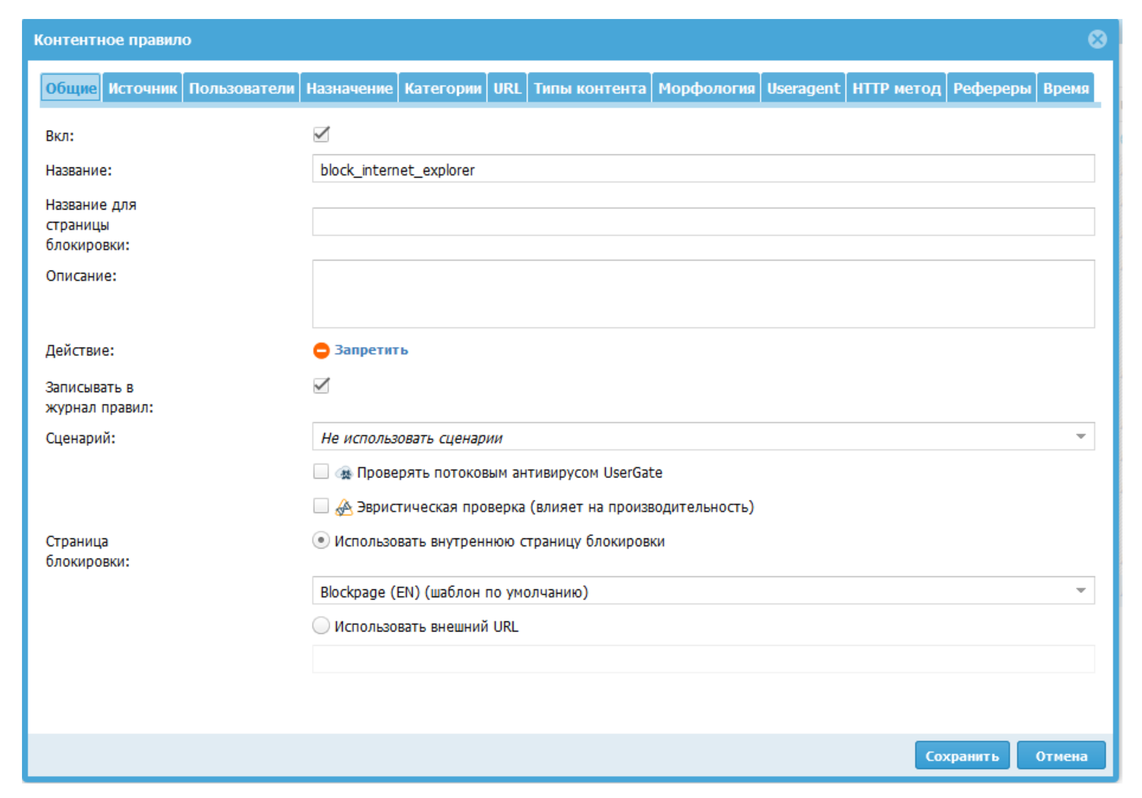


Рисунок Б.18. Настройка правил фильтрации

2. Морфология:

• Добавление морфологического словаря для распознавания слов и фраз. Если определенные слова или фразы обнаруживаются в контенте, доступ к сайту блокируется.

3. Useragent:

- Разрешение или блокировка определенных браузеров. Например, можно запретить работу с Internet Explorer.

4. HTTP метод:

- Указание HTTP-метода (например, POST или GET), используемого в запросах.

5. Рефереры:

- Блокировка или разрешение контента для определенных референов (URL, откуда пришел запрос).

Примеры правил:

1. Блокировка ZIP-архивов:

- Создаем правило "Запретить ZIP-архивы" с действием "Запретить" для зоны "Trusted" и на вкладке "Тип контента" добавляем собственный тип "application/zip". Теперь скачивание ZIP-архивов будет заблокировано.

2. Блокировка Internet Explorer:

- Создаем правило "Блокировать Internet Explorer" на вкладке "Useragent", выбираем Internet Explorer. Теперь любая попытка использовать Internet Explorer для просмотра страниц будет блокирована.

3. Блокировка по морфологическому словарю:

- Создаем правило "Блокировка по слову Банк" на вкладке "Морфология", добавляем слово "Банк" в свой собственный словарь. Теперь страницы, содержащие это слово, будут заблокированы.

4. Работа с HTTP Реферами:

- Создаем правило "Разрешить Tssolution.ru CDN" выше правила блокировки CDN. На вкладке "Рефереры" добавляем URL "tssolution.ru". Теперь сайт будет работать, несмотря на блокировку CDN.

Важно соблюдать последовательность правил, чтобы избежать конфликтов. При большом количестве условий необходимо тщательно настраивать порядок правил для эффективной фильтрации контента.

Исследуем раздел "Веб-безопасность" в системе UserGate, фокусируясь на включении дополнительных параметров для протоколов HTTP и HTTPS, при условии активированного инспектирования HTTPS (рисунок Б.19).

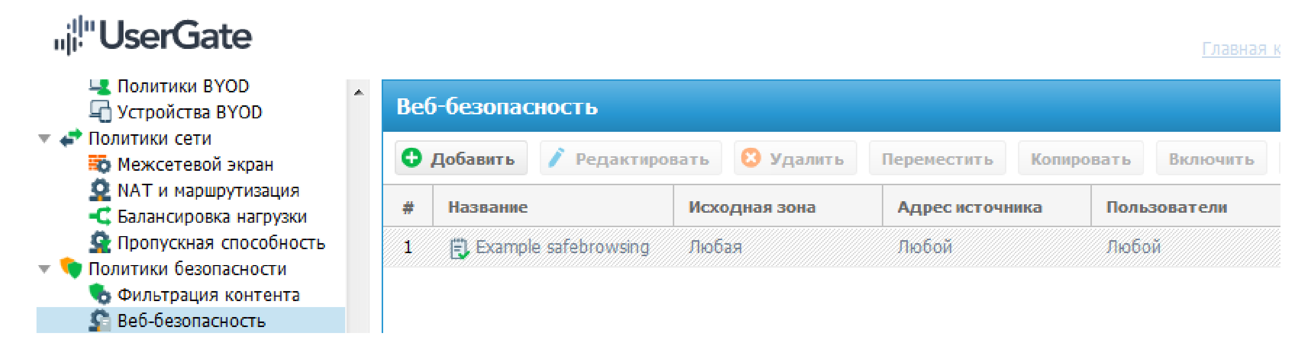


Рисунок Б.19. Раздел «Веб-безопасность»

Параметры Веб-безопасности (рисунок Б.20):

1. Блокирование Рекламы:

- UserGate включает в себя встроенный механизм удаления рекламы, избавляя пользователей от необходимости устанавливать дополнительные плагины в свои браузеры. Это обеспечивает более чистый и эффективный пользовательский опыт, освобождая интерфейс от раздражающих рекламных элементов.

2. Инжектирование Скрипта:

- Функция "Инжектировать скрипт" позволяет вставлять необходимый код во все веб-страницы, просматриваемые пользователем. Соответствующий скрипт будет вставлен в код веб-страниц перед закрывающим тегом `</head>`. Это предоставляет администратору дополнительные возможности для внедрения пользовательских скриптов или

кода для обеспечения дополнительной безопасности.

3. Безопасный Поиск:

- Функция "Безопасный поиск" обеспечивает принудительное включение безопасного поиска для различных поисковых систем, таких как Google, Yandex и YouTube, где это возможно. Это улучшает безопасность пользователя при поиске в интернете, блокируя потенциально опасные результаты.

4. История Поиска:

- Чекбокс "История поиска" предоставляет возможность включить журналирование поисковых запросов пользователей. Это полезный инструмент для анализа и мониторинга активности пользователей, что может быть ценным с точки зрения безопасности и управления ресурсами.

5. Блокировка Приложений Социальных Сетей:

- Этот параметр предоставляет возможность блокировать приложения социальных сетей, не влияя на основную функциональность самих социальных сетей. Например, это может быть использовано для блокировки игровых приложений в социальных сетях, обеспечивая более продуктивное использование сетевых ресурсов.

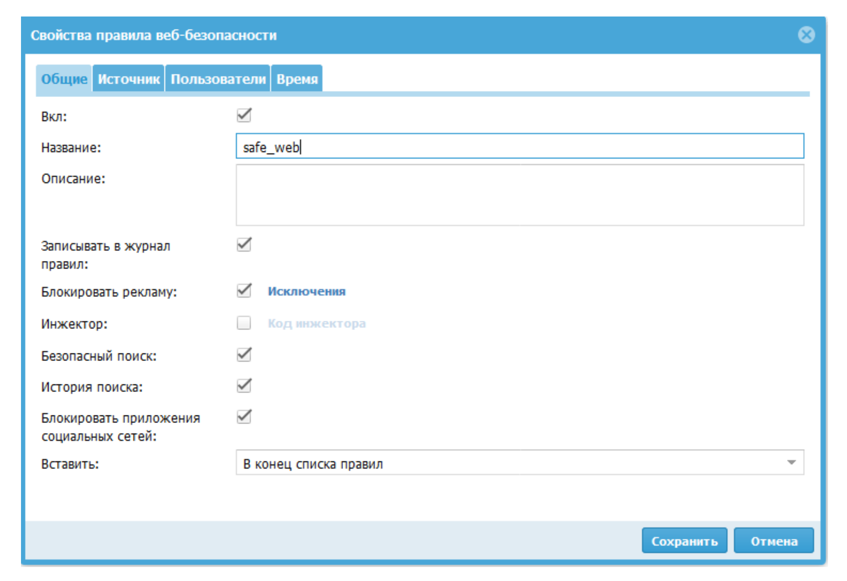


Рисунок Б.20. Свойства правил веб-безопасности

Сфокусируемся на настройке Remote Access VPN и SSL VPN, предоставляя детальные шаги для обоих подходов.

Remote Access VPN (рисунки Б.21- Б.25):

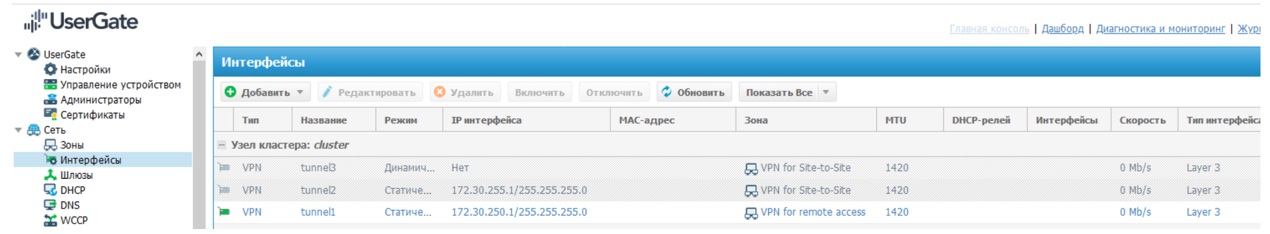


Рисунок Б.21. Интерфейс настройки VPN

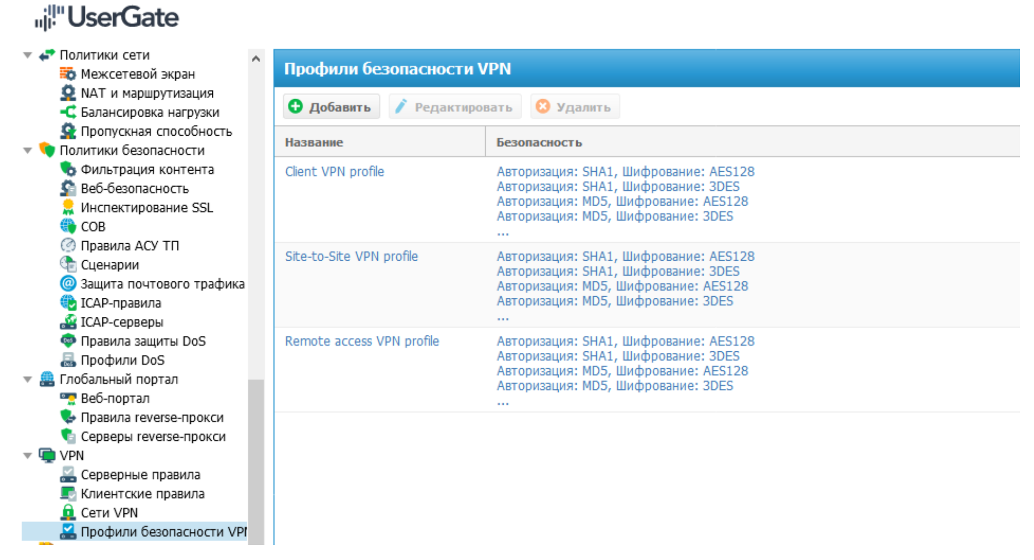


Рисунок Б.22. Профили безопасности VPN

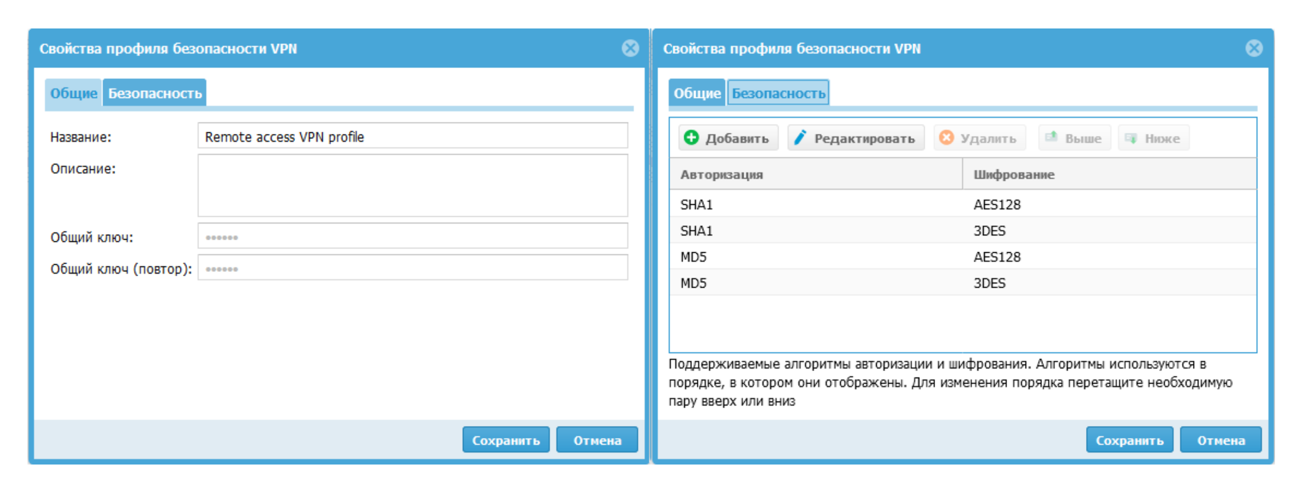


Рисунок Б.23. Настройка профиля безопасности VPN

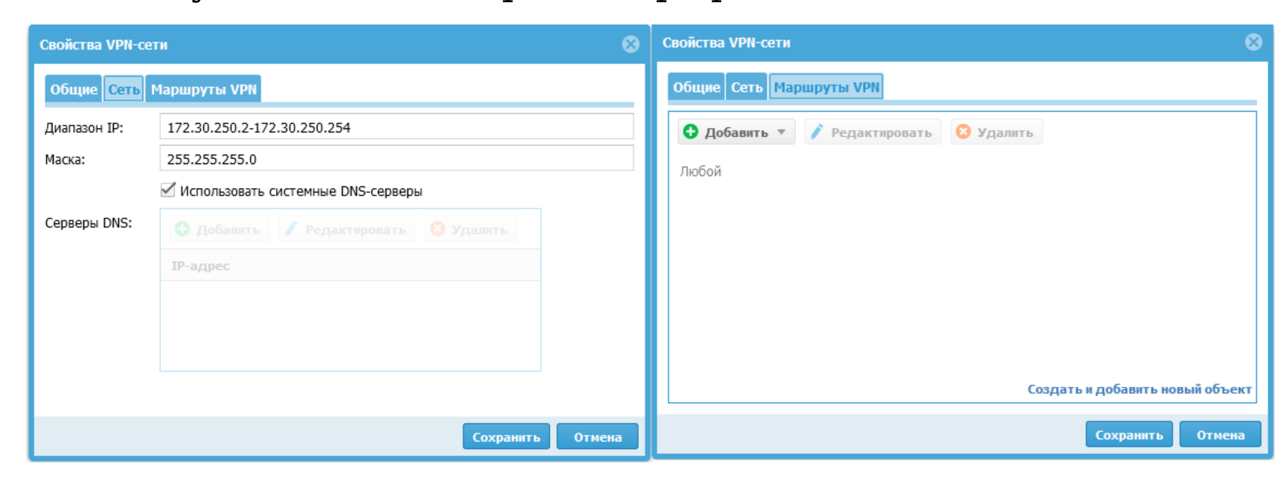


Рисунок Б.24. Настройка VPN-сети

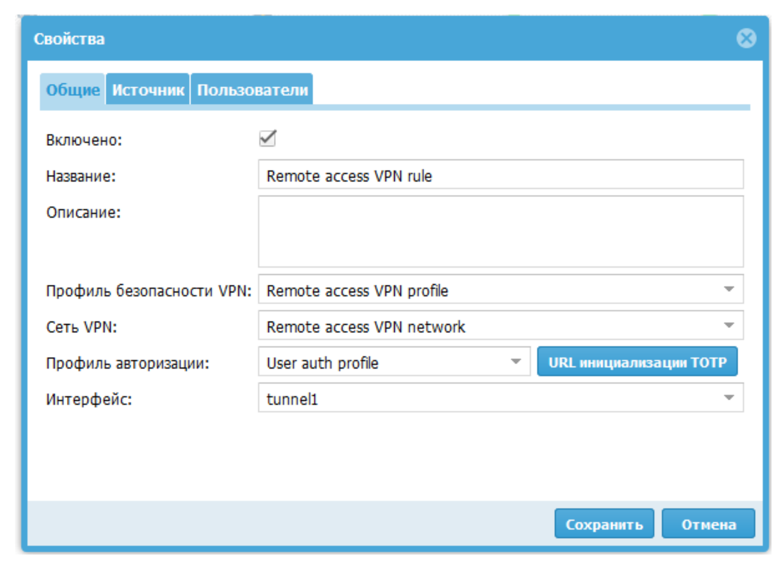


Рисунок Б.25. Результаты настройки MFA TOTP

1. Настройка Сервера:

- UserGate использует протокол Layer 2 Tunnelling Protocol (L2TP) в сочетании с протоколом IPSec для создания туннелей VPN. В разделе "Сеть" разрешаем сервис VPN для

соответствующей зоны, например, "Untrusted".

- Создаем зону "VPN for remote access", предназначенную для клиентов, подключаемых через VPN.

2. Настройка Правил NAT:

- Создаем правило NAT для направления трафика из зоны "VPN for remote access" в нужные зоны, например, "Trusted" и "Untrusted".

3. Настройка Правил Межсетевого Экрана:

- Включаем существующее правило "VPN for remote access to Trusted and Untrusted" в разделе "Политики сети" или создаем новое, разрешая трафик между "VPN for remote access" и "Trusted" и "Untrusted".

4. Создание Профиля Авторизации:

- В разделе "Пользователи и устройства" создаем профиль авторизации, не используя методы прозрачной авторизации, такие как Kerberos или NTLM.

5. Настройка VPN-Интерфейса:

- Переходим в раздел "Сеть" -> "Интерфейсы" и включаем VPN-интерфейс, например, tunnel1, рекомендованный для Remote Access VPN.

6. Конфигурация Параметров VPN:

- В разделе "VPN" -> "Профили безопасности VPN" открываем преднастроенный профиль "Remote access VPN profile". На вкладке "Общие" меняем общий ключ шифрования (Preshared key).

Таким образом, подход Remote Access VPN в UserGate предоставляет клиентам безопасный доступ к внутренним ресурсам компании через зашифрованный туннель. Успешная настройка включает в себя создание зоны для VPN, правил NAT и межсетевого экрана, а также конфигурацию

профиля безопасности VPN.

UserGate также поддерживает SSL VPN, предоставляя возможность подключения к внутренним ресурсам через браузер. Однако, не все типы ресурсов могут быть настроены для доступа через SSL VPN.

Настройки SSL VPN включают в себя параметры, такие как блокировка рекламы, инжектирование скрипта, безопасный поиск и блокировка приложений социальных сетей.

Настройка профилей безопасности VPN:

1. Открытие и Изменение Профиля:

- В разделе "Профили безопасности VPN" выбираем преднастроенный профиль "Remote access VPN profile".
- На вкладке "Общие" изменяем общий ключ шифрования (Preshared key).
- На вкладке "Безопасность" выбираем пары алгоритмов аутентификации и шифрования. Алгоритмы используются в порядке, указанном сверху вниз, и устанавливается первая поддерживаемая пара сервером и клиентом.

2. Дополнительные Профили:

- UserGate позволяет иметь несколько профилей, что полезно при подключении различных типов клиентов VPN.

Настройка Сетей VPN:

3. Создание или Изменение Сети VPN:

- В разделе "Сети VPN" создаем новую сеть VPN или изменяем существующую, например, "Remote access VPN network".
- Назначаем диапазон IP-адресов для клиентов, исключая адреса VPN-интерфейса, и устанавливаем DNS-

сервера или используем системные DNS.

- На вкладке "Маршруты VPN" указываем маршруты в формате CIDR для передачи клиентам. Например, указываем только локальную сеть для маршрутизации трафика.

4. Создание Серверного Правила:

- В разделе "Серверные правила" создаем серверное правило, используя ранее настроенные сеть VPN, интерфейс VPN, профиль VPN, зону "Untrusted", профиль авторизации "User auth profile" и указываем пользователей VPN.

5. Настройка MFA (при необходимости):

- Если требуется многофакторная авторизация (MFA) TOTP, производится инициализация TOTP-устройства в данном разделе.

6. Настройка Клиента:

- Настройка VPN клиента на пользовательском компьютере, учитывая особенности, такие как использование незашифрованного пароля (PAP) для Windows 10.

Настройка на Linux Клиентах (рисунки Б.26- Б.27):

7. Дополнительные Пакеты:

- На Linux клиентах устанавливаются пакеты network-manager-l2tp и network-manager-l2tp-gnome.

8. Настройка VPN-Подключения:

- Создание нового VPN-подключения, выбрав Layer 2 Tunneling Protocol (L2TP).
- Указание параметров аутентификации, метода PAP, и настройка параметров IPsec.



Рисунок Б.26. Выбор Layer 2 Tunneling Protocol (L2TP)

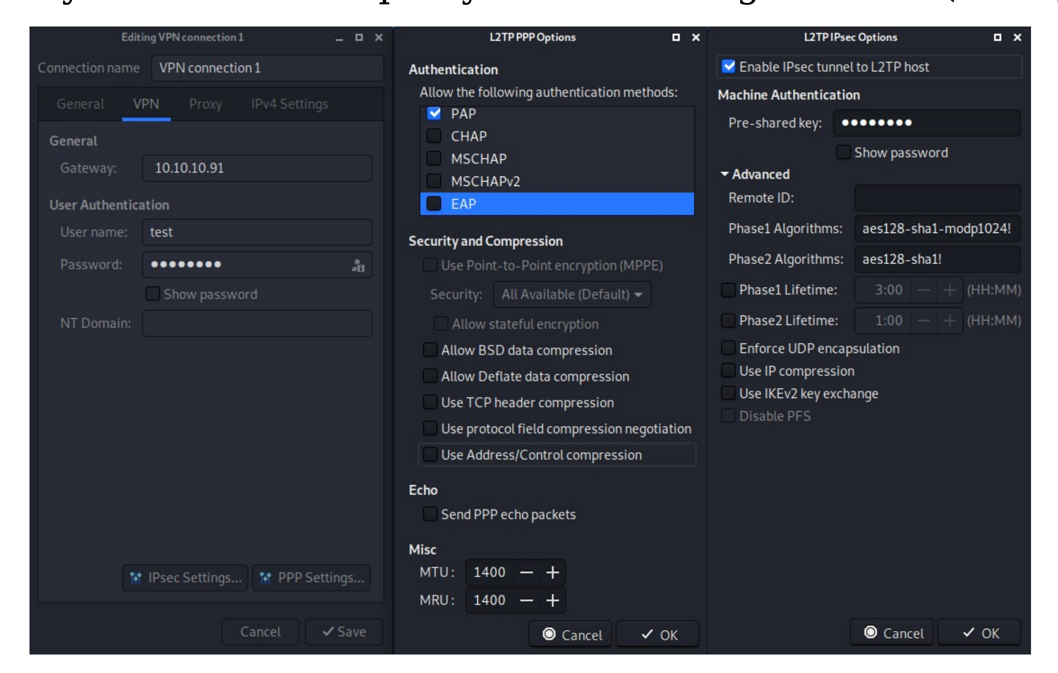


Рисунок Б.27. Настройка параметров подключения и указывание данных для аутентификации

Веб-портал (SSL VPN) (рисунки Б.28- Б.29):

9. Включение Веб-Портала:

- В разделе "Настройки" активируем веб-портал, указываем имя хоста, порт, профиль авторизации, шаблоны страниц и необходимые настройки, включая SSL сертификат.

10. Добавление Внутренних Ресурсов:

- В разделе "Глобальный портал" -> "Веб-портал" создаем записи для внутренних ресурсов, указывая URL, иконки, и параметры доступа.

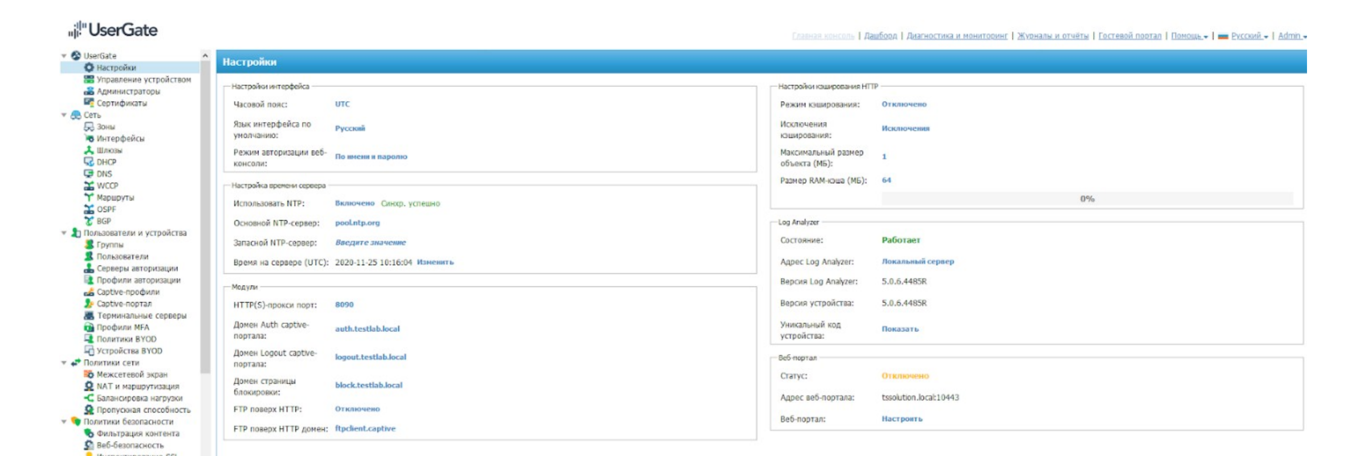


Рисунок Б.28. Включение Веб-Портала

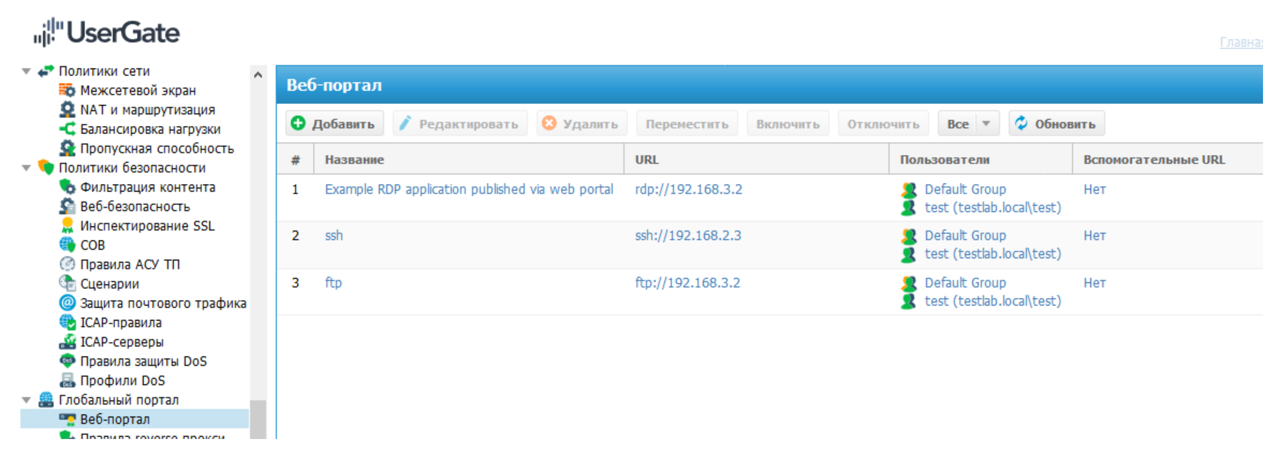


Рисунок Б.29. Добавление Внутренних Ресурсов

ПОСЛЕДНИЙ ЛИСТ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Выпускная квалификационная работа выполнена мной совершенно самостоятельно. Все использованные в работе материалы и концепции из опубликованной научной литературы и других источников имеют ссылки на них.

«_____» ___________________ 202__ г.

_________________________/ Мамонтов Илья Васильевич
(подпись) (Ф.И.О.)

